Supporting LTE Network and Service Management through Session Data Record Analysis

Dániel Kozma, Gábor Soós, Pál Varga

Abstract—**Gathering and processing data for performance and fault management continues to be a burning issue, from LTE operations and maintenance point of view. Regarding the Evolved Packet Core (EPC), this is especially true, since it has newly defined interfaces, with new protocols - some of them are even ciphered. Network-wide data capture and analysis for the EPC requires new processing methods. These would allow operators to correlate control and user plane information of various interfaces and protocols. There are many obstacles to overcome here, including ciphered control messages and global identifiers hidden by temporary ones. This paper presents a system for S1AP session data record assembling, it shows what key parameters are needed to be extracted in order to enable expert analysis. The deciphering mechanism is especially important here, hence we discuss how its success affects analysis results. We present Call Data Record assembling methods for various scenarios - such as network attachments or tracking area changes. Furthermore, this paper presents the methods for gathering cross-correlated data on specific fault management use-cases, especially for unsuccessful voice calls.**

I. Introduction

WIRELESS data traffic is increasing exponentially worldwide [1]. Supporting and managing this growth of traffic on the signaling links poses a great challenge to the operators. Fault management - especially the detection and the root cause analysis of failures - has become very complex, and requires deep telecommunications knowledge. Magyar Telekom - the Hungarian subsidiary of the Deutsche Telekom Group - is facing a milestone in its operation, when introducing voice calls over its 4G network - or in other terms, the Voice over LTE (VoLTE) [2] service. One of the key information-exchange points of 4G call establishment is the S1-MME interface (between eNodeB and MME entities; see Fig. 1). Various important elements of 4G call procedures can be observed at this interface - hence its monitoring is critical from the operator's point of view. On this interface, the role of the S1 Application Protocol (S1AP) [3] is essential when introducing the 4G voice call feature. The monitoring of this interface is important from the Voice over LTE service assurance point of view. Passive monitoring is supposed to be lossless: when the links are tapped, and the probes receive data in a non-intrusive manner, they cannot ask for resending anything. What they missed seeing, they have lost capturing. Based on the monitoring data, engineers can support performance management, network optimization, as well as failure detection, which is one of the most important tasks for operations and maintenance. This paper discusses the requirements and the functions of an S1AP monitoring system, which is under deployment. Furthermore, the paper presents some practical use-cases on call tracing with deciphering issues, as well.

II. Monitoring the LTE Evolved Packet Core

Before discussing the monitoring requirements, this section briefly summarizes the main functions of LTE EPC nodes, and lists the interfaces among them. Parts of LTE network monitoring are discussed in the scientific community; however papers that are sharing actual methodologies and results appear very rarely. The motivations and fundamental challenges of LTE monitoring are discussed in [8]. The basics of network monitoring applied to LTE core system monitoring are summarized in [9]. In [10] the authors describe protocol decoders for LTE, and raise similar issues that our current paper raises and solves.There are also descriptions availale for complete performance management solutions for the backhaul [12] and for end-to-end services [11] – these use the results of LTE EPC monitoring systems, for which an example is presented in the current paper. A CDR synthesis-system for the S1-MME interface is described in [13] – this system shares the fundamentals with the SGA system described in the following sections.

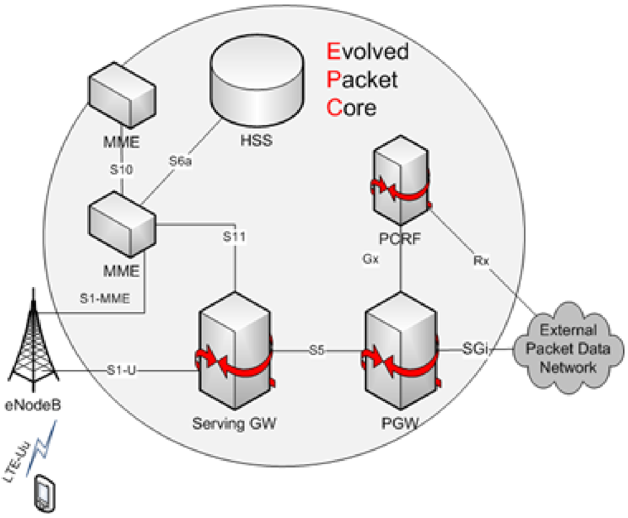


Fig. 1. The architectural elements and interfaces of the LTE EPC

Manuscript received May 25, 2016, revised June 24, 2016.

D. Kozma and G. Soós are with Magyar Telekom Plc. H-1117 Budapest, Szerémi út 4. e-mail: kozma.daniel@telekom.hu, soos.gabor2@telekom.hu

P. Varga is with Budapest University of Technology and Economics, Department of Telecommunications and Media Informatics H-1117 Budapest, Magyar Tudósok körútja 2. e-mail: pvarga@tmit.bme.hu

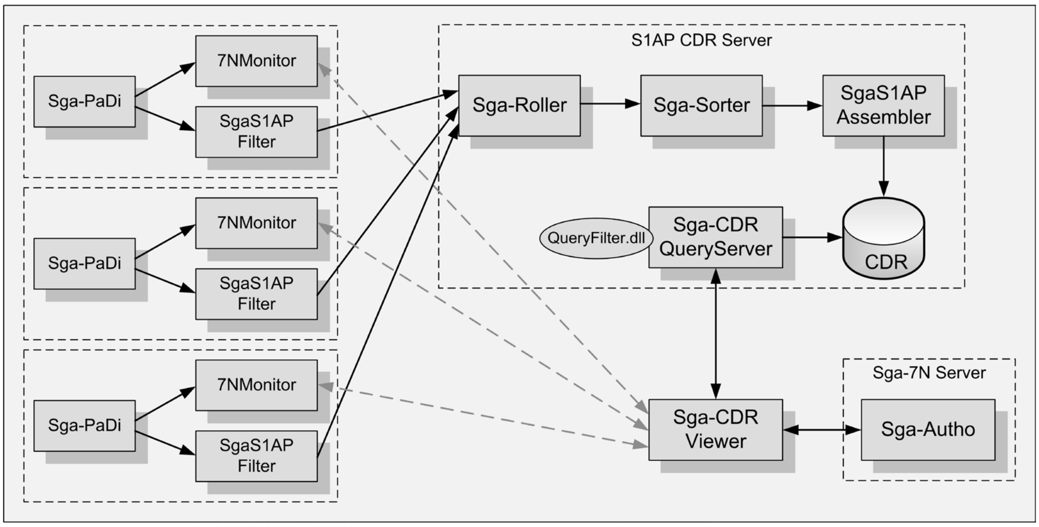


Fig. 2. Monitoring architecture for S1AP CDR creation within the SGA-7N Monitoring System [7]

A. LTE EPC Architecture

The LTE Evolved Packet Core (EPC) [4] comprises merely packet switched network elements; it only supports the legacy circuit switched functions through IP-based packet transfer. Fig. 1 depicts the architecture of the LTE Evolved Packet Core - and the defined interfaces in between its elements.

MME (Mobility Management Entity): The MME lies on the border of the EPC and EUTRAN (Evolved Universal Mobile Telecommunications System Terrestrial Radio Access Network) - and is mainly responsible for mobility-management. Its main functions include controlling handovers between eNodeBs (Evolved NodeB, Base Station), SGW (Serving Gateways) or MMEs, connecting to HSS (Home Subscriber Server), user identification, authentication and controlling the roaming functions. MME registers and handles the User Equipment (UE) in his own area, registers where the UE is located, either exactly at eNodeB level (if communication is active), or within a Tracking Area (TA), which is designated to a group of eNodeBs (in case of passive UE, no active connection is needed).

SGW (Serving Gateway): The SGW is responsible for user traffic stream handling, and controlling the allocation of resource capacities, the changes or deletion of sessions and finishing IP connections. From the eNodeB point of view, it is a fix, anchor node through which the core network elements can be accessed. Furthermore, the SGW controls the User Plane tunnels with GPRS Tunneling Protocol (GTP) [5], although this can be also guided by the MME or the PGW - depending on the process rules.

PGW (Packet Data Network Gateway): PGW can be seen as an edge node of the EPC, since it ensures the connections to external data networks (e.g., the Internet or a private corporate network) and handles the UE's data traffic that is entering or leaving the core network. Besides, it offers interfaces for further functions such as QoS control or billing.

HSS (Home Subscriber Server): HSS takes the roles of HLR/AuC (Home Location Register/Authentication Centre) in the LTE network. It can be seen as the ultimate data storage that contains the subscribers' service-related data. The HSS stores the subscribers' profile, containing the enabled services and access (e.g. allowed roaming services to external networks). It is mainly responsible for access management and authentication, and it also registers the subscribers' position within the network. The HSS cooperates with the MME in all UE-related change events that are administered by the EPC.

PCRF (Policy and Charging Rules Function): Based on its predefined policies and QoS-related rules, the PCRF sends control information to the PGW. This piece of information is called "Policy Control and Charging rules", and it is exchanged between the PCRF and the PGW when a new bearer is set up, e.g. in case new UE activates new PDP to the network or a new UE requires a data plane bearer with a different QoS policy.

B. Monitoring functions

The core network of Magyar Telekom is overseen by the SGA-7N network monitoring system, developed by AITIA International Inc.[6]. The main aim of this monitoring is failure detection and analysis. Further uses include generating key performance indicators on network segments and servicing scenarios, detecting and real-time filtering of fraudulent cases, assembling session- and call-data records for further analysis. The special hardware of the monitoring probes connects to all sorts of network interfaces from E1 to Multi-Gigabit Ethernet, and it also ensures high-precision time-stamping. Lossless traffic capture and real-time data processing and traffic analysis are key features of network monitoring. The connection is passive (non-intrusive), and control-plane traffic is collected bit-by-bit; then, it is stored and pre-processed to allow further analysis. The monitoring system creates signaling statistics, session- and call-data records, allows run real-time call tracing based on the collected data, and enables post-processing for further investigations.

III. SESSION DATA RECORDS OF THE S1AP INTERFACE

The S1AP-CDR system is part of the SGA-7N monitoring systems. It assembles records from the S1AP traffic, the control messages exchanged between the eNodeBs and MMEs. The architectural view of the functional elements for CDR-creation can be seen in Fig. 2.

When capturing the traffic, the Sga-PaDi (Packet Distributor) on the monitoring probes passes the packets to the SgaS1APFilter module for separating the non-S1AP traffic traversing on the link. The messages are collected by the Roller function, which combines the messages arriving from different monitors. During the next step, the Sorter receives the records where the traffic will be ordered - based on timestamp. Thanks to the buffer before and after the Sorter, this part can be stopped and started anytime without losing any packets. The chronologically ordered packets are transferred to the Assembler, where S1AP-CDR records get generated. In order to avoid data loss before stopping the Assembler, status saving is required. With this, we can also avoid disturbing transient effects during the restart. The generated S1AP-CDR records then become readable and searchable also.

A. S1AP CDR Assembling

In order to understand the necessities of CDR assembly we have to look into the details of "Filter" and "Assembler".

SgaS1AP Filter: The Filter is aimed to decrease the traffic between the nodes with passing over merely the relevant packets. This module receives traffic from Sga-PaDi, separates Paging and non-Paging messages from the S1AP traffic and generates groups from Paging messages. The filtered S1AP traffic is forwarded to the SgaRoller and logs in .csv format the counters periodically (e.g. every 15 minutes).

SgaS1AP Assembler: This module owns the advanced logic of assembling session data records from individual messages [7]. It selects the processable S1AP messages and associates them with each other, by using their contained identifiers: mme-ue-s1ap-id and enb-ue-s1ap-id. The S1AP connection can be clearly identified between the MME and eNodeB - based on these parameters, within a specific time-range. It associates the S1AP/Paging messages to the connections using the M-TMSI (MME-Temporary Mobile Subscriber Identity). The associated messages are written into records, together with the corresponding IMSI. This latter association comes from the information gathered from the central Key-Servers, which connect ciphering keys and IMSIs from S6a, as well as Gr and Gn interfaces. The internal processes of CDR assembling can be fully traced with the help of internal counters, which are logged and recorded as 15 min records in .csv format.

B. Presentation of S1AP CDRs

The CDR Viewer is the visualization part of the Sga-7N network monitoring system. The database can be searched with different parameters of various protocols, including BSSAP/RANAP, SGsAP, S1AP and GTP. The main features are the following:

- by default only the basic CDR parameters are shown,
- the CDR details appear when clicking on the chosen record,
- presentation can be configured so that it shows or hides various traffic parameters,
- changes can be saved to ASCII TEXT, CSV, RTF and HTML format,
- sophisticated authentication in the hidden attributes.

With the "Get messages" request, the messages that were assembled together for the CDR get shown in a protocol decoder view (which also has a bit-by-bit viewer). This function is provided by the Sga Message Viewer, the ultimate protocol decoder that belongs to the monitoring system.

C. Ciphering issues

During the S1-MME interface monitoring it is very helpful for the operators to be able to search exactly the IMSI and to show all corresponding control messages. To do this we also need to decrypt the encryption on the interface. Currently, commercial 4G voice calls are not supported in the Magyar Telekom network yet, CS fallback is used instead for handling calls. To do this, the UE has to change radio access type to 3G or 2G. This is hard to monitor mainly because the encryption keys are transmitted inside the combo MME-SGSN node. Monitoring the outside interfaces of the Core nodes, GTP, MAP (Mobile Application Part) and DIAMETER messages are received and by saving all IMSI-key exchange, these encryptions can be cleared [7]. The decryption and ordering of different encryptions is a complex problem. To validate the final solution AITIA [7] implemented a specific software tool for manual decryption, that can be used with the help of the proper, saved keys. The software requires the following parameters, based on an "Attach" event [4]:

- CK (Ciphering Key), IK (Integrity Key), AUTN (Authentication Key)
- MCC (Mobile Country Code), MNC (Mobile Network Code): basic network identifiers,
- Based on the identifiers calculating the KASME
- Integrity and ciphering algorithm (based mainly on EIA1/EEA1)
- Input: the file which we want to decrypt
- Output: where we would like to save the results
- check MAC (Medium Access Control) and decode: validation and decoding

To decrypt the TAU (Tracking Area Update) messages we need different parameters, after the IK and CK, NonceMME and NonceUE parameters are also requested (see Fig. 3). Let's examine some cases where is a need to use the encryption keys, and to use the SGA4MD software to find the user records on the S1AP interface [8].

First Example, Basic event

User attaches to the 4G network and the MME requires a key [7].

1, On the HLR-HSS connection SAI (Send Authentication Info) messages originating from the MME should be searched.

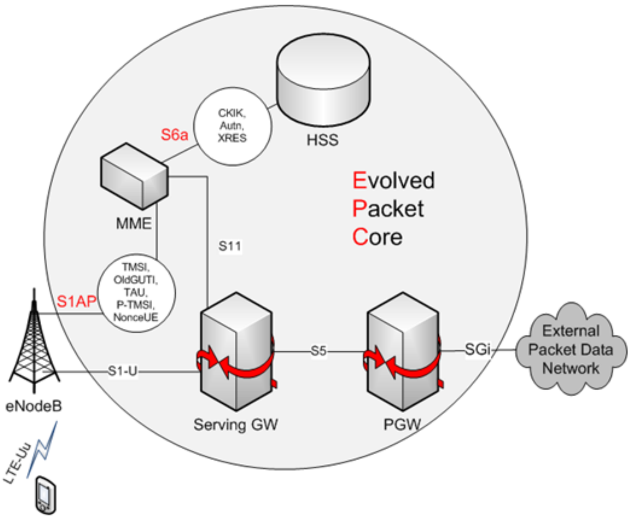


Fig. 3. LTE Authentication and Key Agreement - S1AP and S6a parameters

2, On the S1AP the attached messages should be paired; the easiest way is to search the appropriate XRES (Expected Response) in the ACRS (Accounting Requests) messages.
3, To get the full ACRS, choose the full S1AP dialog.

Second example, Attach case

User connects to 4G, but SGSN-MME receives the key earlier during a 3G attach. In some cases the key cannot be seen because of the combined SGSN-MME node. The original key-exchange can be monitored merely on the SGSN-HLR MAP connection [7].

1, On S1AP, Attach messages should be searched. These contain two kinds of TMSIs (Temporary Mobile Subscriber Identifier). Choose the one in the "Old GUTI"(Globally Unique Temporary ID).
2, Search for this on GTP among the "SGSN Ctxt" and "Identity" messages. For this example, the Identity message should be searched. It is possible that there is no match, again, because of the combined SGSN-MME.
3, Choose the whole S1AP dialogue of the Attach.
4, If there is ACRS among the messages, the new key should be searched (a) in GTP messages, or (b) in the HLR-HSS connection. The authentication vector can be found based on XRES; and the KASME can be calculated.
5, For the first part of the S1AP message exchange the first key, whereas for the last part of the S1AP message exchange the second key should be used.
6, It is not easy to find the original key: the M-TMSI sharing is encrypted on S1AP, hence it cannot be read.
7, In order to decrypt, the GTP search should be based on GTP-TEID filter; the "Create"-s according to IMSI and the search for those TEIDs on the S1AP should be issued.

Third example, Tracking Area case

1, There can be at least two kinds of searches: either (a) "SGSN ctxt transfer" search on GTP, or (b) TAU search on S1AP.
(a) Let's search on the GTP SGSN ctxt transfer to the MME direction. The search is not trivial, because we can see also the 3G-3G change [7]. The solution is to check the MME-SGSN nodes, because they have different IP addresses, so the filtering of the search is simplified.
(b) To filter the search for those TAUs on S1AP, we need such TAUs that have the same NAS Key Set ID.
2, Based on the earlier two cases (a) and (b), we have to search the messages travelling through the other protocol. This time - similarly to the Attach-case - we need the retransformed P-TMSI (Packet-Temporary Mobile Subscriber Identifier) from the Old GUTI.
3, Based on the actual keys seen on the GTP (CK, IK) and the TAU message containing the NonceUE parameter, the KASME key can be derived. In case of Handover, the Sec Mode command message is necessary, because it contains NonceU and NonceMME fields together.

IV. Analysis methods for S1AP CDRs

In some cases, the S1AP CDRs are assembled irregularly; this is marked by the assembler through writing error-messages. These have to be investigated. In order to carry out the investigation, deep knowledge is needed about the network architecture, the S1AP protocol itself, and some experience of the S1AP collecting software's operation. In the following we demonstrate some typically irregular scenarios of the CDR assembly procedure.

Incomplete - Release

Cases belonging here start with "Incomplete" and close with "Release" messages of the S1AP CDR assembling procedure. During the process, we receive packets after the closed connection, which was not included into the CDR#1 - and a new record was opened for CDR#2. The message was received very close in time to the DelayedClosedTimeout, but not exceeding eg. DelayedClosedTimeout = 5s. As an example: a lot of messages were received within 4,947s. After changing DelayedClosedTimeout = 6s, we decreased the number of such irregularities with one magnitude - which is a good result [7].

Incomplete - Error

Further investigating the cases of messages starting with Incomplete, we focused on the CDRs closed with "error". In case of Incomplete-Error CDRs, the CDR#1 completion is prevented by a different CDR, because the eNodeB-MME reference IDs got modified. During the investigation we found, that although the IDs got modified, later we have received messages with the original reference IDs. After modifying the assembling procedure to hold the old IDs for a longer period, the problem was eliminated.

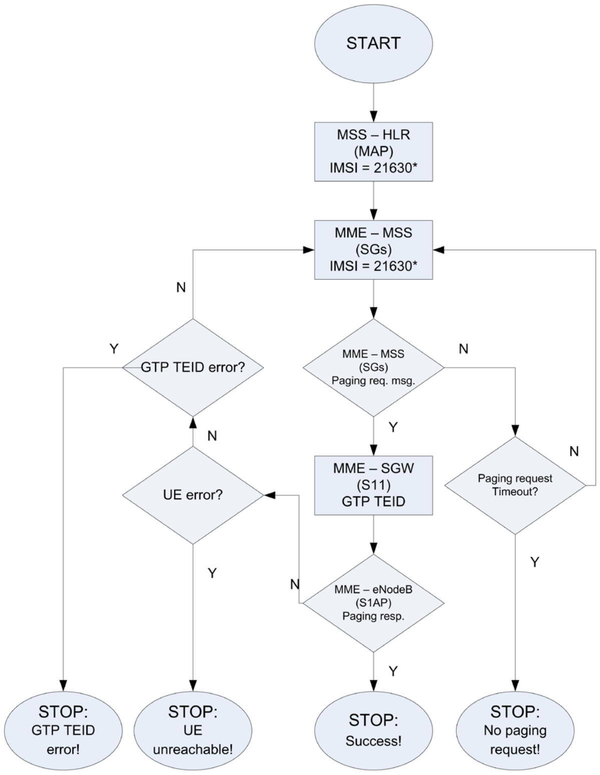


Fig. 4. Workflow of the call analysis.

No Paging

Some S1AP CDRs were opened with "No paging", which means they opened without an initial paging. Based on the standard this should not happen, because at the first step of S1AP establishment the MME sends paging to the eNodeB, based on the M-TMSI. The irregular CDR assembling procedure looked like the following: during a not-closed transaction, the eNodeB sent an InitialUEMessage to the MME. (The InitialUeMessage is normally the second message after the paging, and its purpose is to establish the data connection between the UE and the core network). In the examined cases there were no initial paging messages, because there was an active, not-closed connection. This resulted in a seemingly irregular CDR assembly scenario. There are two conclusions of this example: (1) it validates the right behavior of the CDR creation, because such cases are not standard, and (2) it occurs only in few cases, meaning that this can be caused by user equipment error.

V. Use Cases

Compared to the examined calls we should investigate the control traffic on the most important links. During these calls we know only one identifier in the beginning - such as the MSISDN. The first step is to find messages that carry that identifier (in the given time-range), and then to look for further, important, maybe temporary identifiers within those messages. In the further steps we can then initiate searches for those temporary identifiers, to find the corresponding S1AP signaling information.

A. Everything is normal

As a first case we present a successful call scenario. Since we know the MSISDN, the IMSI can be found in the MSS-HLR link, as can be seen in the output depicted by Fig. 5. In the next step, the GTP identifiers were collected - based on IMSI - in the MME-SGW interface. Thanks to the GTP identifiers, the required signaling packets can be matched on the S1 interface. As the output shows, the paging was successfully sent.

B. Erroneous case

In this example our test voice-call was unsuccessful: it got forwarded to voice-mail, however we know the user was reachable during that time. Regarding the operator's work, the search was similar to the previously illustrated case. At first, we found the IMSI on the MSS-HLR link (by using the MSISDN and the time as the search criteria), then based on the GTP identifier, we found an interesting message (see typesetted, timestamped).

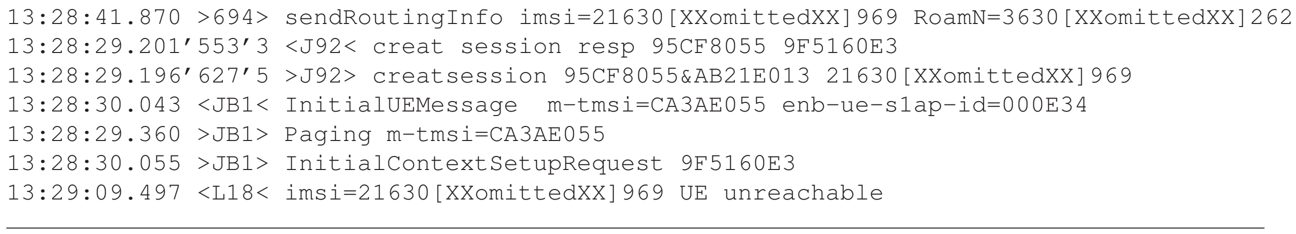
Paging was sent, but still we received an "Ue unreachable" message. There can be many reasons for this, including UE failure, loss of coverage, etc.. Although this method helps us to investigate a lot of similar issues, the greatest problem still remains the parallel search on a lot of links. This requires a lot of time, and not just tens of minutes but even some hours could be needed for a proper examination.

C. Automating the fault management process

The analysis of one complete call includes data gathering and investigation from all the links that can be associated with the different aspects of call establishment. This requires a lot of time and deep knowledge of the system interfaces. Investigation of one failure requires hours of work; however with S1AP monitoring, we will have the opportunity to get all data from the links at once - by only knowing one identifier. Automating this requires of course some development, but it makes the work of the operator's engineers more comfortable and effective. Fig. 4 presents an automated analysis method, where one request can fire off sequential, automated operations. This starts with only one known parameter (IMSI), and provides a trace result that includes all related messages. Analysis time can be decreased with at least one order of magnitude – when compared to the above described, mostly by using a manual method that involves the intensive usage of the CDR Viewer.

VI. Conclusion

This paper is focusing on monitoring and analysis of the Evolved Packet Core (EPC), in order to provide traffic analysis methods for the Voice over LTE service. After briefly summarizing the elements of the LTE EPC, we briefly discussed the requirements and a solution for network-wide traffic monitoring in the core. Furthermore, there are some



```
13:28:41.870 >694> sendRoutingInfo imsi=21630[XXomittedXX]969 RoamN=3630[XXomittedXX]262
13:28:29.201’553’3 <J92< creat session resp 95CF8055 9F5160E3
13:28:29.196’627’5 >J92> creatsession 95CF8055&AB21E013 21630[XXomittedXX]969
13:28:30.043 <JB1< InitialUEMessage  m-tmsi=CA3AE055 enb-ue-s1ap-id=000E34
13:28:29.360 >JB1> Paging m-tmsi=CA3AE055
13:28:30.055 >JB1> InitialContextSetupRequest 9F5160E3
13:29:09.497 <L18< imsi=21630[XXomittedXX]969 UE unreachable
```

Fig. 5. Signalling on the MAP interface

issues brought up due to the ciphering of most of the S1AP messages; these need to be deciphered, for which the proper keys are required to be collected and utilized. Handling this is a difficult engineering problem, because we have to know the contexts between the protocols, keys and identifiers. We have presented a method for S1AP session data record assembling, the key parameters and the general method for their assembly. As a main part of the paper, we have showed methods on how to extract valuable information from these CDRs for various use cases, including basic events, attach cases or tracking area related cases. Furthermore we showed analysis methods for S1AP CDRs for incomplete, or other erroneous cases, and analysis use cases when the operator only knows a single identifier (such as the MSISDN), and a time range to search in. We presented the methods how to gather cross-correlated data on specific fault management use-cases, especially for unsuccessful voice calls. It is clear, that some of these analysis steps can and should be made automatic: we suggest further development in that direction, too. Developing the network monitoring system in parallel with the rising expectations of the customers is very important here.

Acknowledgment

The authors would like to thank to AITIA’s engineers – especially Gábor Sey and Gábor Szelindi –, for their support.

References

[1] CISCO - "Cisco Visual Network Index Global Mobile Data Traffic Forecast Update 2014-2019", 2015.

[2] Miikka Poikselkä, Harri Holma, Jukka Hongisto, Juha Kallio, Antti Toskala - "Voice over LTE (VoLTE)", John Wiley & Sons, 2012.

[3] 3GPP TS 36.413 V10.9. - "Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP)", Release 10, 2014.

[4] M.Olsson, S. Sultana, S.Rommer, L.Frid, C. Mulligan - "EPC and 4G Packet Networks, Second Edition, 2013.

[5] 3GPP TS 29.060 V10.12.0 - "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp interface", Release 10, 2015.

[6] Pál Varga, Gábor Szelindi, Gábor Sey, Endre Cseszkó - "Az LTE maghálózat monitorozásának kihívásai és megoldásai" (The challenges and solutions of LTE core network monitoring), Híradástechnika Magazin, pp.36-42, LXVII, 2012.

[7] Gábor Sey, Gábor Szelindi - "Monitoring S1AP", Interim Report, AITIA, 2015.

[8] Bachar Wehbi1, Jouko Sankala, Edgardo Montes de Oca - "Network Monitoring Challenges in the Evolved Packet Core", Future Network and Mobile Summit, 2012.

[9] Wu Cuixian, Wang Shengnan, Liu Zhiguang - "The Signaling Monitoring Scheme of LTE System", Instrumentation, Measurement, Computer, Communication and Control (IEEE-IMCCC), 2013.

[10] M. Manjula, G. Varaprasad - "Implementation of Decoders for LTE Interface Messages", International Conference on Networking and Distributed Computing (ICNDC), 2011.

[11] Li Li, Subin Shen - "End-to-End QoS performance management across LTE networks", Asia-Pacific Network Operations and Management Symposium (IEEE-APNOMS), 2011.

[12] Charlie Chen-Yui Yang, Michael Ketcham, David Lu, David Kinsey - "Performance Monitoring with Predictive QoS Analysis of LTE Backhaul", Cyber-Enabled Distributed Computing and Knowledge Discovery (IEEE CyberC), 2011.

[13] Zhen Li, Zhi Zhang Zhang, Di Ran - "Research and Implementation of CDR Synthesis Scheme on S1-MME Interface in LTE Network", Advanced Materials Research (Volumes 926-930), Chapter X. Communications and Information Technology Applications, 2014.

Gábor Soós received his M.Sc. degree in Electrical Engineering from Budapest University of Technology and Economics (BME), Hungary, in 2008. He joined T-Systems Corp. in 2008 and has been involved in radio network modeling as well implementation for reliable advanced radio communication technologies. Currently, he is responsible for Magyar Telekom Core network developement and investigation of advanced process technologies, current interests advanced mobile networks and testing of highly realible core systems.

Dániel Kozma received the MSc degree in Electrical Engineering from BME, Budapest, Hungary, in 2015. He joined Magyar Telekom, Hungary, in 2014. His main areas of interest are Mobile Network Signaling-Monitoring, IMS Development and Subscriber Data Management. Daniel is currently a member of an international team which was created by the Magyar Telekom and Deutsche Telekom, and his main tasks are IMS application-implementation and database management.

Pál Varga is Associate Professor at BME, Hungary, where he got his M.Sc. (1997) and Ph.D. (2011) degrees from. Besides, he is director in AITIA International Inc. Earlier he was working for Ericsson Hungary and Tecnomen Ireland, as software design engineer and system architect, respectively. His main research interest include communication systems, network performance measurements, root cause analysis, fault localisation, traffic classification, end-to-end QoS and SLA issues, as well as hardware acceleration, and Internet of Things.