Sharevski *EURASIP Journal on Information Security* (2018) 2018:8
https://doi.org/10.1186/s13635-018-0078-7

EURASIP Journal on
Information Security

REVIEW Open Access

Towards 5G cellular network forensics

Filipo Sharevski

Abstract

The fifth generation (5G) of cellular networks will bring 10 Gb/s user speeds, 1000-fold increase in system capacity, and 100 times higher connection density. In response to these requirements, the 5G networks will incorporate technologies like CUPS, NFV, network slicing, and CIoT. Each of these 5G features requires system adaptations to enable acquisition and forensic processing of cellular network evidence. This paper reviews the digital forensics mechanisms for Lawful Interception and user localization available in LTE and LTE-Advanced networks together with the associated evidence types, tools for forensic analysis, and supporting legal framework. The challenges and potential adaptations for retaining these capabilities in the future 5G networks are also discussed to outline the future research directions for cellular network forensics.

Keywords: Cellular networks, LTE/LTE-Advanced, 5G, Lawful Interception (LI), Lawful Access Location Services (LALS)

1 Introduction

Cellular networks evolved through four generations and the fifth is projected for commercial roll-out in 2022. Currently, there are 7.5 billion worldwide cellular subscriptions, each generating 5 GB of traffic per month on average [1]. The subscription and traffic volume is forecast to increase fivefold in the next 5 years, requiring 5G to accommodate 1000 times the system capacity of the current LTE/LTE-Advanced networks. The pervasiveness of cellular access implies that most crimes are, or will be, facilitated by cellular devices. To support legal processing, cellular network forensic investigations are necessary in obtaining critical evidence, especially in cases where it is infeasible to physically seize a cellular device or a critical transient data is needed promptly [2].

Cellular network forensics is a cross-discipline of digital forensics and cellular networks with the goal to investigate *cellular network-facilitated crimes* under a legally obtained warrant for the purpose of crime reconstruction. These criminal activities can be carried out with a direct network support (e.g., perpetrators communicate over a cellular network) or network is incidental to the crime (e.g., the network can provide historical data about calls or user locations). The investigations in cellular network can be in real time and non-real-time. The real-time investigations work with evidence transiting over the network at the time of the crime or the attack like ongoing calls, browsing sessions, or triangulated geolocation coordinates of a user. The non-real-time investigations work with evidence in relation to past user activity such as charging data records or user's most visited cell. Prior to every investigation, operators and law enforcement agencies (LEAs) must establish forensic readiness to ensure secure identification, acquisition, and delivery of cellular network evidence [3, 4]. These operations are realized with two forensics mechanisms, *Lawful Interception* (LI) and *Lawful Access Location Services* (LALS).

This article reviews the implementation of LI and LALS in LTE and LTE-Advanced networks. Various types of LI and LALS evidence are also presented together with tools and techniques for cellular network forensic analysis. The challenges for continuous support of LI and LALS are discussed in the context of the key technologies for 5G evolution including Control and User Plane Separation (CUPS), Network Functional Virtualization (NFV), network slicing, and CIoT. Several adaptations of the current LI and LALS operations for each 5G technology are proposed and elaborated to ensure the future cellular network forensic investigations are conducted as similarly as possible to the current practice. The article concludes with a discussion of the legal and privacy aspects of the current and future cellular network forensics practice.

Correspondence: fsharevs@cdm.depaul.edu
College of Computing and Digital Media, DePaul University, 243 S Wabash Ave, Chicago, IL 60610 USA

2 LTE cellular network forensics

2.1 Lawful Interception

LI refers to the legally provisioned action performed by a cellular network operator to make the communication and the communication-related information available to one or more LEA [5]. Figure 1 shows the LI architecture for LTE/LTE-Advanced networks. Every LI is invoked for a *target identity,* e.g., suspected user or victim, and/or a *target service,* e.g., all outgoing data and SMSs. The target identity is specified with either a MSISDN, IMSI, IMEI, or a combination of them. To distinguish between different LI requests, the Law Enforcement Monitoring Facility (LEMF) uses a unique LIID. This information together with the time period for interception and the delivery information is sent over the HI1. Every operator has an internal Administration Function (ADMF) that takes the requests, provisions the LI to the Interception Control Elements (ICEs), and configures the IP addresses of the delivery interfaces.

The example shown in Fig. 1 depicts interception of all outgoing data and SMS, so in this case ADMF provisions LI at the MME, S/P-GW, and the SMSC [6]. Operators can intercept two types of cellular data: *user traffic* and *signaling traffic*. The intercepted user traffic is referenced as *Content of Communication (CC)* and delivered over the HI3 in a pre-defined format to the LEMF (e.g., audio or pcap files). The intercepted signaling traffic is referenced as *Interception-Related Information (IRI)* and is delivered over the HI2 in various IRI record types.

All interfaces use a specific LI protocol implementation, shown on Fig. 2. The LI application layer is responsible for authentication and encrypted delivery of the administrative messages, the IRI records, and the CC. The LI session layer encapsulates the IRI records and CC data before it sends them over a TCP/IP connection so the LEMF can distinguish between different LI application messages. The encapsulation is realized using the ITOT protocol over port 106 [7].

2.1.1 Interception-Related Information (IRI)

There are four types of IRI records that the network can provide to the LEA:

- IRI-BEGIN—The first event of a communication attempt of the target identity
- IRI-END—The end of a communication attempt; closing the IRI transaction for the targeted identity and/or service
- IRI-CONTINUE—Intermediary record at any time during a communication within the IRI transaction
- IRI-REPORT record—Used for non-communication-related events, for example, a network attach request

The IRI records and CC data need to be correlated for a given target identity. For that purpose, each IRI record contains a unique *correlation number*. In addition, the IRI records contain information about

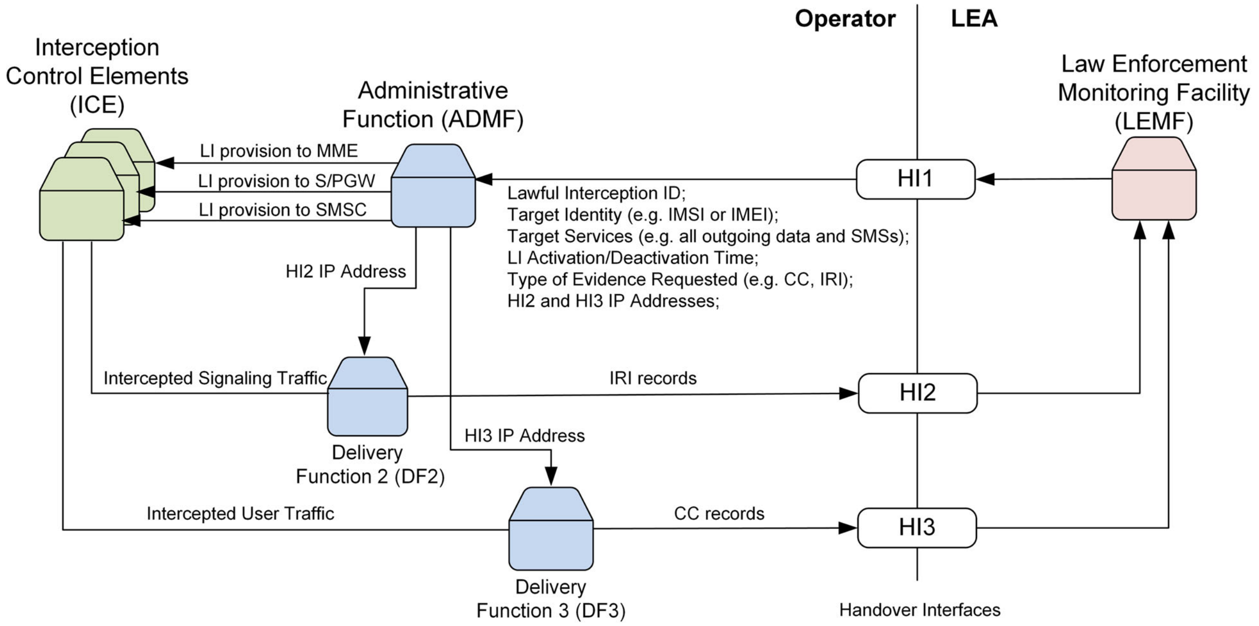

Operator
LEA
Interception Control Elements (ICE)
Administrative Function (ADMF)
Law Enforcement Monitoring Facility (LEMF)
LI provision to MME
LI provision to S/PGW
LI provision to SMSC
HI1
Lawful Interception ID;
Target Identity (e.g. IMSI or IMEI);
Target Services (e.g. all outgoing data and SMSs);
LI Activation/Deactivation Time;
Type of Evidence Requested (e.g. CC, IRI);
HI2 and HI3 IP Addresses;
HI2 IP Address
Intercepted Signaling Traffic
IRI records
HI2
Delivery Function 2 (DF2)
HI3 IP Address
Intercepted User Traffic
CC records
HI3
Delivery Function 3 (DF3)
Handover Interfaces

Fig. 1 The LTE/LTE-Advanced LI architecture. The handover interfaces between the operators and the LEA enable both real-time and non-real-time cellular network evidence identification, acquisition, and delivery

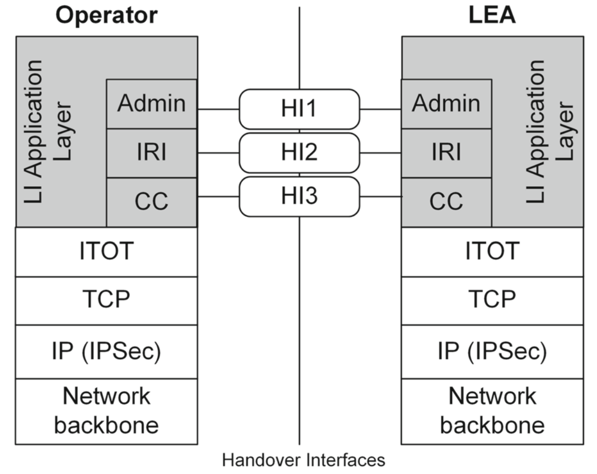


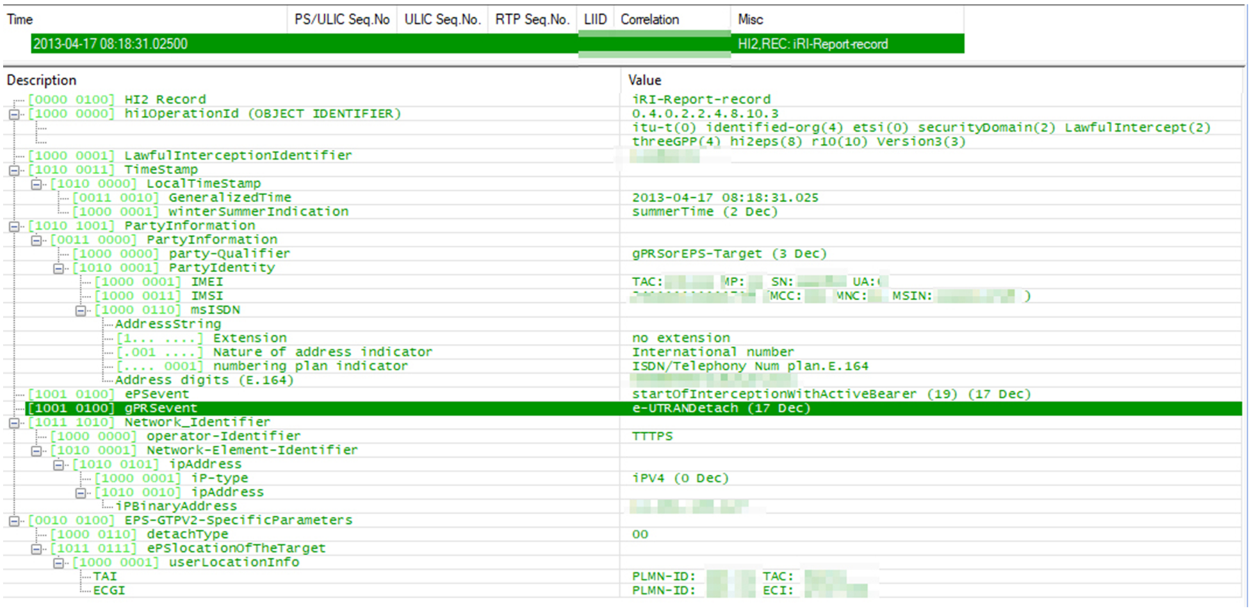
Fig. 2 The LI protocol stack. The encryption and authentication keys used on the LI application layer are negotiated during the forensic readiness phase between the operators and the LEA

the observed MSISDN/IMSI/IMEI, source/destination IP address, source/destination ports, APNs, dialed and connected numbers, serving cell(s), TAI, SMS sender/receiver, SMS content, and date/times/duration of the interception events [6]. An example of IRI-REPORT record for an EUTRAN detach event processed with the STINGA LI-Analyzer tool is shown in Fig. 3 [8]. The intercepted signaling traffic indicates the time and date (LocalTimeStamp attribute) when the target identity initiated the network detach (gPRSevent and detachType attribute), either by switching off the cellphone, battery loss, or removing the SIM card.

For non-real-time investigations, investigators have the alternative to use the IRI records in conjunction with the charging data records (CDRs) generated by each ICE for charging purposes. The CDRs contain similar information as the IRI records and are often used in investigations because they can be obtained offline from the operators. An example of an originating SMS CDR used in plotting a location with Google Earth and the TraX software is shown in Fig. 4 [9]. In this case, the CDR shows the time, date, and the location where the target identity was registered when sending a SMS of interest (operator usually supplies the coordinates of their base stations so the LEA can infer the location from the LAC/CID parameters). This information can be verified with the IRI record associated with the same event, which can further reveal the content of the originating SMS (usually sent as part of the signaling traffic).

2.1.2 Content of Communication (CC)

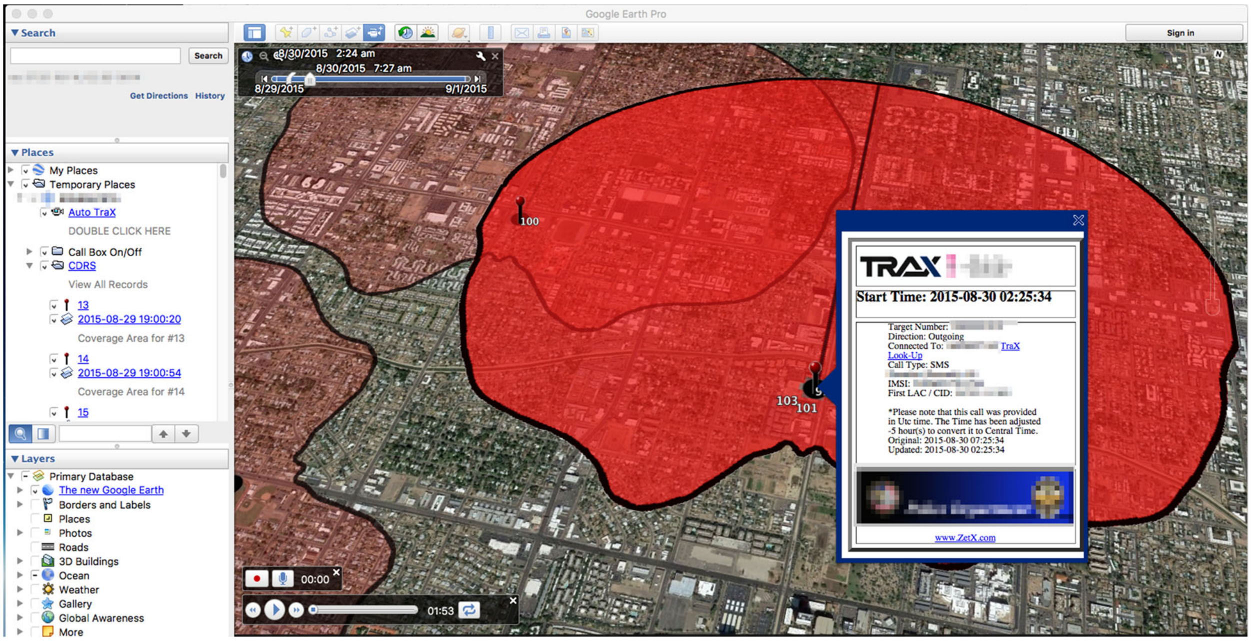
The CC data represents the actual user traffic that is realized over the cellular network by the target identity. It includes actual voice conversations intercepted and delivered in formats like .wav files or IP sessions delivered in packet captures like .pcap files. To determine whether the conversational parties from the intercepted voice CC are the ones subject to investigation, various *forensic speaker recognition* techniques are used to analyze the voice CC. The aural/acoustic technique relies on experienced



```
Time                     PS/ULIC Seq.No  ULIC Seq.No.  RTP Seq.No.  LIID  Correlation  Misc
2013-04-17 08:18:31.02500                                                 [redacted]   HI2,REC: iRI-Report-record

Description                                                   Value
[0000 0100] HI2 Record                                        iRI-Report-record
[1000 0000] hi1OperationId (OBJECT IDENTIFIER)                0.4.0.2.2.4.8.10.3
                                                              itu-t(0) identified-org(4) etsi(0) securityDomain(2) LawfulIntercept(2)
                                                              threeGPP(4) hi2eps(8) r10(10) Version3(3)
[1000 0001] LawfulInterceptionIdentifier                      [redacted]
[1010 0011] TimeStamp
  [1010 0000] LocalTimeStamp
    [0011 0010] GeneralizedTime                               2013-04-17 08:18:31.025
    [1000 0001] winterSummerIndication                        summerTime (2 Dec)
[1010 1001] PartyInformation
  [0011 0000] PartyInformation
    [1000 0000] party-Qualifier                               gPRSorEPS-Target (3 Dec)
    [1010 0001] PartyIdentity
      [1000 0001] IMEI                                        TAC:[redacted] MP:[redacted] SN:[redacted] UA:[redacted]
      [1000 0011] IMSI                                        [redacted] MCC:[redacted] MNC:[redacted] MSIN:[redacted] )
      [1000 0110] msISDN
        AddressString
        [1... ....] Extension                                 no extension
        [.001 ....] Nature of address indicator               International number
        [.... 0001] numbering plan indicator                  ISDN/Telephony Num plan.E.164
        Address digits (E.164)                                [redacted]
[1001 0100] ePSevent                                          startOfInterceptionWithActiveBearer (19) (17 Dec)
[1001 0100] gPRSevent                                         e-UTRANDetach (17 Dec)
[1011 1010] Network_Identifier
  [1000 0000] operator-Identifier                             TTTPS
  [1010 0001] Network-Element-Identifier
    [1010 0101] ipAddress
      [1000 0001] iP-type                                     iPV4 (0 Dec)
      [1010 0010] ipAddress
        iPBinaryAddress                                       [redacted]
[0010 0100] EPS-GTPV2-SpecificParameters
  [1000 0110] detachType                                      00
  [1011 0111] ePSlocationOfTheTarget
    [1000 0001] userLocationInfo
      TAI                                                     PLMN-ID: [redacted] TAC: [redacted]
      ECGI                                                    PLMN-ID: [redacted] ECI: [redacted]
```

Fig. 3 IRI-REPORT record for an EUTRAN detach event. This is an original IRI record from a cellular network investigation so the correlation number, LLID, IMEI, IMSI, MSISDN, IP address, TAI, and ECGI are blurred to protect the anonymity of the target identity



TRAX [redacted]

Start Time: 2015-08-30 02:25:34

Target Number: [redacted]
Direction: Outgoing
Connected To: [redacted] TraX Look-Up
Call Type: SMS
[redacted]
IMSI: [redacted]
First LAC / CID: [redacted]

*Please note that this call was provided in Utc time. The Time has been adjusted -5 hour(s) to convert it to Central Time.
Original: 2015-08-30 07:25:34
Updated: 2015-08-30 02:25:34

[redacted]

www.ZetX.com

Fig. 4 A CDR for an LTE voice call. This is an original CDR from a non-real-time cellular network investigation so the MSISDN, IMSI, LAC, and CID are blurred to protect the anonymity of the target identity

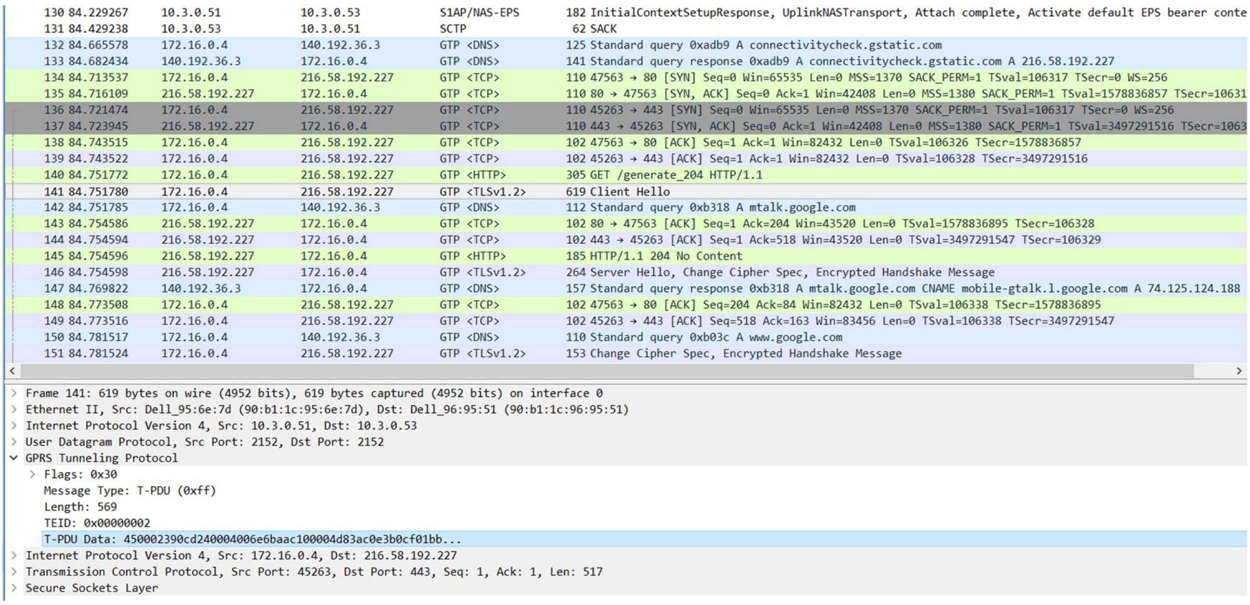
human perception in matching the intercepted voice CC and a recorded voice based on the phonetic similarity between the two sources [10]. The auditor-instrumental technique employs statistical analysis of common voice features like the average fundamental frequency, articulation rate, formant central frequencies, rhythm, and voice quality to determine for the same purpose. In the automatic forensic speaker recognition, the recognition system works by extracting voice features of a training set of speech data to model different speaker patterns that are later compared with the features extracted of the intercepted voice CC to yield a similarity score with the target speaker. Among the most prominent tools for automatic forensic speaker recognition is ALIZE [11].

For the IP CC data, the analysis of the packet captures is performed using standardized tools and techniques for regular network forensics processing, e.g., Wireshark. Figure 5 shows a Wireshark capture of DNS query and a HTTPS session establishment encapsulated in a GTP tunnel. The CC data in this case is correlated with an IRI-BEGIN record to indicate the beginning of the user IP traffic, IRI-CONTINUE records for the duration of the session or the interception, and IRI-END records when the user closes its session or the interception is terminated (the correlation number for the CC is not shown in the figure but is supplemented over the HI3 interface and is similar to the one present on the IRI records).

2.2 Lawful Access Location Services—LALS

LALS refer to the legally provisioned action performed by a cellular network operator to make location information available to one or more LEAs. Cellular networks provide Location Services (LCS) that utilize the geographic location of the user (i.e., advertising or an emergency localization). For this purpose, cellular networks implement a LCS architecture with LMUs in the radio network to execute the localization measurement and SMLCs in the core network to communicate the location information with the LCS clients. SMLCs communicate the localization requests using the LPP protocol to the LMUs, which in turn coordinate with the target identities to calculate their current location. This location information can be provided to external entities, for example LEAs. The user location is calculated using either of these localization methods [12]:

- ECID—The coordinates of the cellular device are derived by measuring either the RTT or the AoA of a reference signal between one or three base stations and the cellular device (known also as *triangulation*). The precision of the ECID positioning is between 50 m and 1 km, but the Time-To-First-Fix (TTFF) is less than a few seconds for more than 90% accuracy.
- OTDOA—The mobile device measures the TOA for the downlink reference signals received from multiple base stations (at least three) and subtracts it



```
130 84.229267   10.3.0.51      10.3.0.53      S1AP/NAS-EPS   182 InitialContextSetupResponse, UplinkNASTransport, Attach complete, Activate default EPS bearer conte
131 84.429238   10.3.0.53      10.3.0.51      SCTP            62 SACK
132 84.665578   172.16.0.4     140.192.36.3   GTP <DNS>      125 Standard query 0xadb9 A connectivitycheck.gstatic.com
133 84.682434   140.192.36.3   172.16.0.4     GTP <DNS>      141 Standard query response 0xadb9 A connectivitycheck.gstatic.com A 216.58.192.227
134 84.713537   172.16.0.4     216.58.192.227 GTP <TCP>      110 47563 → 80 [SYN] Seq=0 Win=65535 Len=0 MSS=1370 SACK_PERM=1 TSval=106317 TSecr=0 WS=256
135 84.716109   216.58.192.227 172.16.0.4     GTP <TCP>      110 80 → 47563 [SYN, ACK] Seq=0 Ack=1 Win=42408 Len=0 MSS=1380 SACK_PERM=1 TSval=1578836857 TSecr=10631
136 84.721474   172.16.0.4     216.58.192.227 GTP <TCP>      110 45263 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1370 SACK_PERM=1 TSval=106317 TSecr=0 WS=256
137 84.723945   216.58.192.227 172.16.0.4     GTP <TCP>      110 443 → 45263 [SYN, ACK] Seq=0 Ack=1 Win=42408 Len=0 MSS=1380 SACK_PERM=1 TSval=3497291516 TSecr=1063
138 84.743515   172.16.0.4     216.58.192.227 GTP <TCP>      102 47563 → 80 [ACK] Seq=1 Ack=1 Win=82432 Len=0 TSval=106326 TSecr=1578836857
139 84.743522   172.16.0.4     216.58.192.227 GTP <TCP>      102 45263 → 443 [ACK] Seq=1 Ack=1 Win=82432 Len=0 TSval=106328 TSecr=3497291516
140 84.751772   172.16.0.4     216.58.192.227 GTP <HTTP>     305 GET /generate_204 HTTP/1.1
141 84.751780   172.16.0.4     216.58.192.227 GTP <TLSv1.2>  619 Client Hello
142 84.751785   172.16.0.4     140.192.36.3   GTP <DNS>      112 Standard query 0xb318 A mtalk.google.com
143 84.754586   216.58.192.227 172.16.0.4     GTP <TCP>      102 80 → 47563 [ACK] Seq=1 Ack=204 Win=43520 Len=0 TSval=1578836895 TSecr=106328
144 84.754594   216.58.192.227 172.16.0.4     GTP <TCP>      102 443 → 45263 [ACK] Seq=1 Ack=518 Win=43520 Len=0 TSval=3497291547 TSecr=106329
145 84.754596   216.58.192.227 172.16.0.4     GTP <HTTP>     185 HTTP/1.1 204 No Content
146 84.754598   216.58.192.227 172.16.0.4     GTP <TLSv1.2>  264 Server Hello, Change Cipher Spec, Encrypted Handshake Message
147 84.769822   140.192.36.3   172.16.0.4     GTP <DNS>      157 Standard query response 0xb318 A mtalk.google.com CNAME mobile-gtalk.l.google.com A 74.125.124.188
148 84.773508   172.16.0.4     216.58.192.227 GTP <TCP>      102 47563 → 80 [ACK] Seq=204 Ack=84 Win=82432 Len=0 TSval=106338 TSecr=1578836895
149 84.773516   172.16.0.4     216.58.192.227 GTP <TCP>      102 45263 → 443 [ACK] Seq=518 Ack=163 Win=83456 Len=0 TSval=106338 TSecr=3497291547
150 84.781517   172.16.0.4     140.192.36.3   GTP <DNS>      110 Standard query 0xb03c A www.google.com
151 84.781524   172.16.0.4     216.58.192.227 GTP <TLSv1.2>  153 Change Cipher Spec, Encrypted Handshake Message

> Frame 141: 619 bytes on wire (4952 bits), 619 bytes captured (4952 bits) on interface 0
> Ethernet II, Src: Dell_95:6e:7d (90:b1:1c:95:6e:7d), Dst: Dell_96:95:51 (90:b1:1c:96:95:51)
> Internet Protocol Version 4, Src: 10.3.0.51, Dst: 10.3.0.53
> User Datagram Protocol, Src Port: 2152, Dst Port: 2152
v GPRS Tunneling Protocol
  > Flags: 0x30
    Message Type: T-PDU (0xff)
    Length: 569
    TEID: 0x00000002
    T-PDU Data: 450002390cd240004006e6baac100004d83ac0e3b0cf01bb...
> Internet Protocol Version 4, Src: 172.16.0.4, Dst: 216.58.192.227
> Transmission Control Protocol, Src Port: 45263, Dst Port: 443, Seq: 1, Ack: 1, Len: 517
> Secure Sockets Layer
```

Fig. 5 A CC record for an LTE DNS and HTTPS user session. The capture is taken from a test LTE network setup using the OAI open-source LTE implementation [25]

from a reference TOA from its serving station (known also as *multilateration*). Each of the RSTD measurements describes a hyperbola or ellipsoid so the intersection of their focus lines provides the coordinates of the cellular device. OTDOA precession is less than 50 m with a TTFF of around 10 s but less than 70% accuracy.

- UTDOA—This is a similar positioning method as OTDOA in which the LMUs measure the time difference of arrival of the uplink reference signals from the cellular device. The advantage of the UTDOA is that it requires minimum device involvement, so it improves the accuracy to more than 90% while retaining the same precision and timing as OTDOA.
- A-GNSS—The standalone navigation based on GPS requires unobstructed line of sight between the user and at least four satellites. Given that most of the time users are indoors and cannot satisfy this requirement, cellular networks assist the users by supplying information about the availability and configuration of GPS satellites. The user then measures the available GPS signals so it can calculate its 3-dimensional coordinates and report them to the SMLC. The precision and timing of the A-GNSS is less than 1 m and TTFF of 35 s, though the accuracy is below 80% because the GPS signals needed might not be always available for measurement (for example, almost 50% of the user calls/sessions are indoors).

The LCS architecture allows for various positioning procedures, depending on the entity initiating the localization request. For example, the network can induce a localization after an emergency attach from a user (referred to as EPC-NI-LR) or if an external client like a LEA requests localization for a target identity (referred to as EPC-MT-LR). External LCS clients can be location-based advertising companies, map services, or Enhanced 911/112 systems. Each external client has to be authorized to use the LCS service by the network and the users. For lawful localization, the LEA needs to obtain a warrant and secure the delivery and storage of the location information for the target identities investigated.

In general, all the procedures follow the logical positioning sequence shown in Fig. 6. The SMLC server communicates the positioning capabilities with the targeted UE and sends additional assistance data (e.g., A-GNSS information for satellites, signal references for OTDOA or UTDOA) so the UE can perform the positioning measurements. These measurements are communicated back to the SLMC in a form of a IRI-REPORT record and, depending on the localization method, provide the information on UE's latitude, longitude, altitude, altitude direction, and, optionally, its relative velocity.

The LALS are invoked in two forensic investigation variants: (1) *target positioning* and (2) *enhanced location for IRI*. The target positioning is used to determine the target's location independently of the services used and can be further invoked either for an *immediate localization*

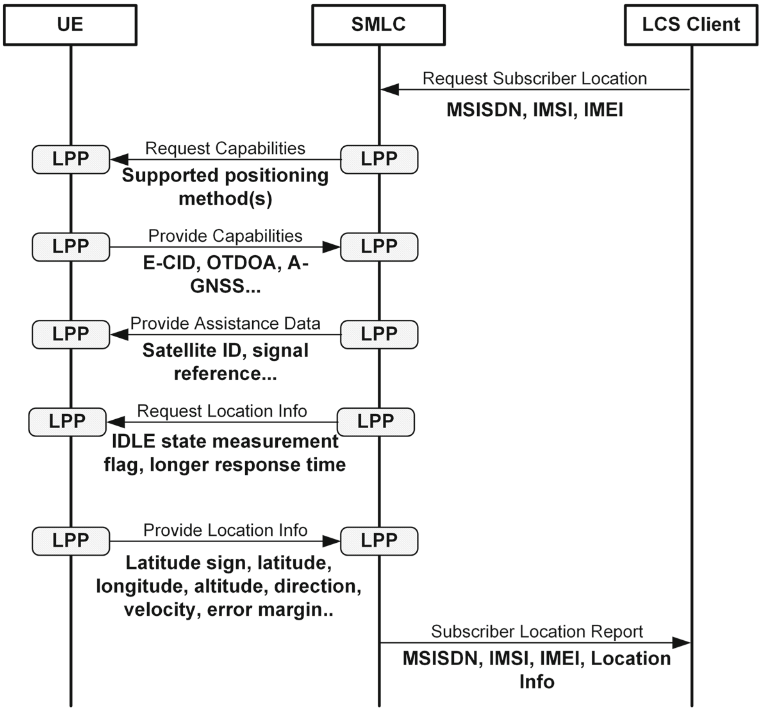

UE
SMLC
LCS Client
Request Subscriber Location
MSISDN, IMSI, IMEI
LPP
Request Capabilities
Supported positioning method(s)
LPP
LPP
Provide Capabilities
E-CID, OTDOA, A-GNSS...
LPP
LPP
Provide Assistance Data
Satellite ID, signal reference...
LPP
LPP
Request Location Info
IDLE state measurement flag, longer response time
LPP
LPP
Provide Location Info
Latitude sign, latitude, longitude, altitude, direction, velocity, error margin..
LPP
Subscriber Location Report
MSISDN, IMSI, IMEI, Location Info

Fig. 6 The general LCS procedure in LTE/LTE-Advanced networks. For LALS-invoked user localization, the LEA is authorized as an LCS client that requests subscribers' (target identity) localization information

or for a *periodic localization*. The immediate localization is invoked when the LEA needs the location of the target in real-time, while the period localization is used in non-real-time cases where the LEA can track the movement of the target identity over a longer period of time. For the periodic localization, the LEA can specify the reporting interval and the number of reports it needs from the SMLC depending on the needed tracking granularity. In cases where the LEA needs to localize a target identity that uses a specific service, e.g., SMS, the enhanced location for IRI is used.

3 Cellular network forensics in 5G

5G is envisioned to achieve 1000 times increase in system throughput, peak data rate of 10 Gb/s, and 100 times higher connection density [13]. The new generation of cellular networks will support new deployment scenarios including high-speed vehicles and trains, IoT, commercial air-to-ground service, and service for light aircraft/helicopters. To meet these requirements, the network architecture introduces a series of novel technologies including CUPS, NFV, network slicing, and CIoT.

3.1 Control and User Plane Separation—CUPS

The idea behind the CUPS is to separate the control and user plane for the S-GW, P-GW, and the TDF. LTE and LTE-Advanced networks already provide separation by implementing most of the control functions in the MME and the user traffic delivery functions in S/P-GW. CUPS takes this separation further to allow independent network scaling—deploying more user plane nodes (e.g., forwarder routers) closer to the network edge without increasing the number of control nodes for applications including tethering, local Vehicle-to-X communications, augmented reality, or optimized video streaming [14].

Figure 7 shows an example of CUPS-based 5G network architecture where the control plane of the S/P-GW elements and the TDF terminate the GTP-C (S5/S8) and Diameter (Gx) protocols. Three new interfaces are introduced in this architecture, Sxa, Sxb, and Sxc, all of which implement the PFCP protocol over UDP/IP. The control elements use PFCP to establish, modify, and delete Sx sessions on the user elements (a user can be served with more than one user element). For this purpose, PFCP allows provisioning of rules like packet detection, forwarding action, QoS enforcement, or usage reporting where each rule is defined in a separate PFD.

From a LI persecutive, CUPS requires some adaptations in the LI function already supported in LTE and LTE-Advanced. The delivery of IRI records in a CUPS deployment is a responsibility of the control elements while the delivery of the CC data responsibility of all user elements serving a target identity. To invoke LI on the network side, ADMF needs to instruct the control elements about

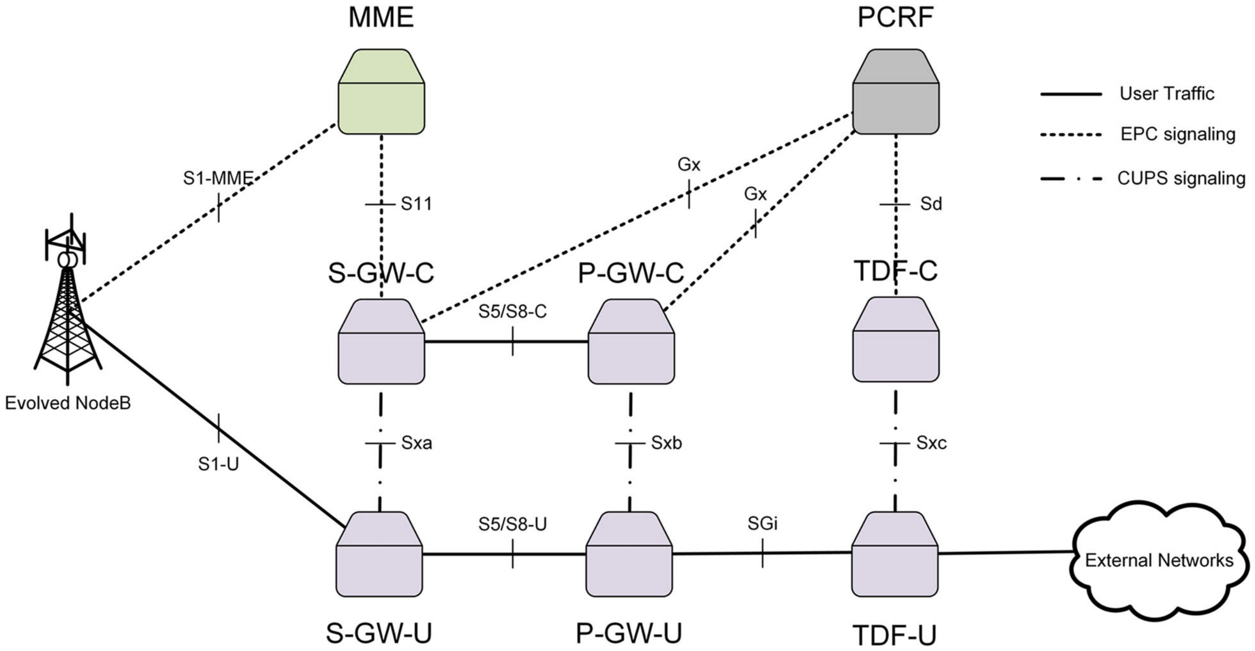


Fig. 7 5G CUPS network architecture. The S-GW and P-GW are split into control elements (S-GW-C and P-GW-C) and user elements (S-GW-U and PG-W-U)

the interception configuration, which in case a CC data is requested, they need to instruct the user elements to route the interception to the DF3. This can be done by defining a new PFD "lawful interception" that is provisioned as a special packet forwarding action to the DF3. Because multiple control elements can be involved in the user traffic delivery, DF3 must be able to consolidate the user traffic before it hands to the HI3 interface using the Sx user session identifier. For the LEA to be able to correlate the IRI and CC for a target identity, DF2 and DF3 have to include the Sx user session identifier in the delivered evidence material. The modified LI architecture including these modifications for a CUPS network deployment is shown in Fig. 8.

From a LALS perspective, the target positioning is not affected with the separation of the control and user planes because the mobility management for LCS is handled separately by the MME and is independent of the cellular service used. Same holds for the enhanced location for IRI, given that each user is served by only one control node

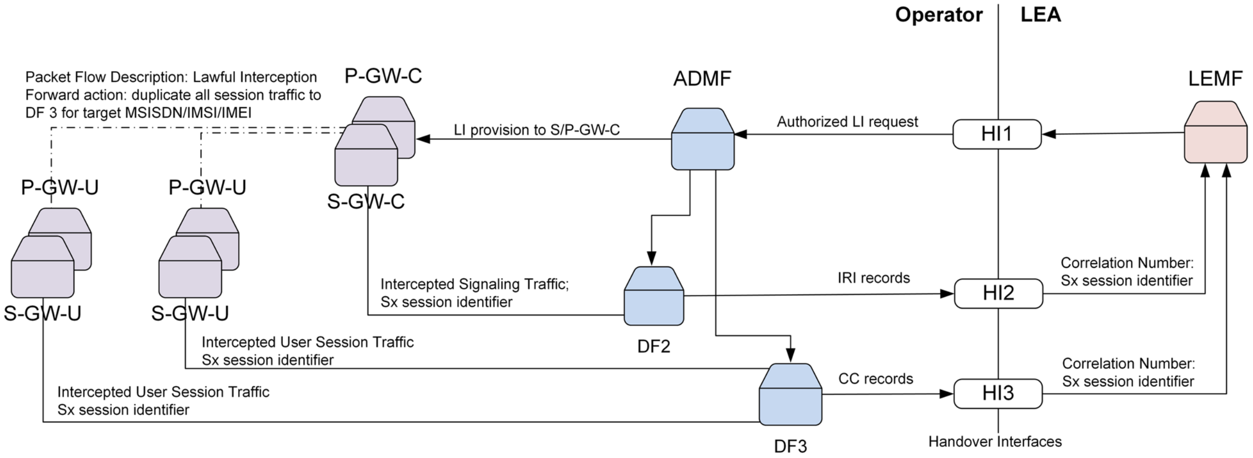


Fig. 8 Modifications in the LI architecture for CUPS support. The essential functionality is preserved for acting on authorized requests from the LEA with adaptions for using the Sx session identifiers as correlation numbers for IRI and CC

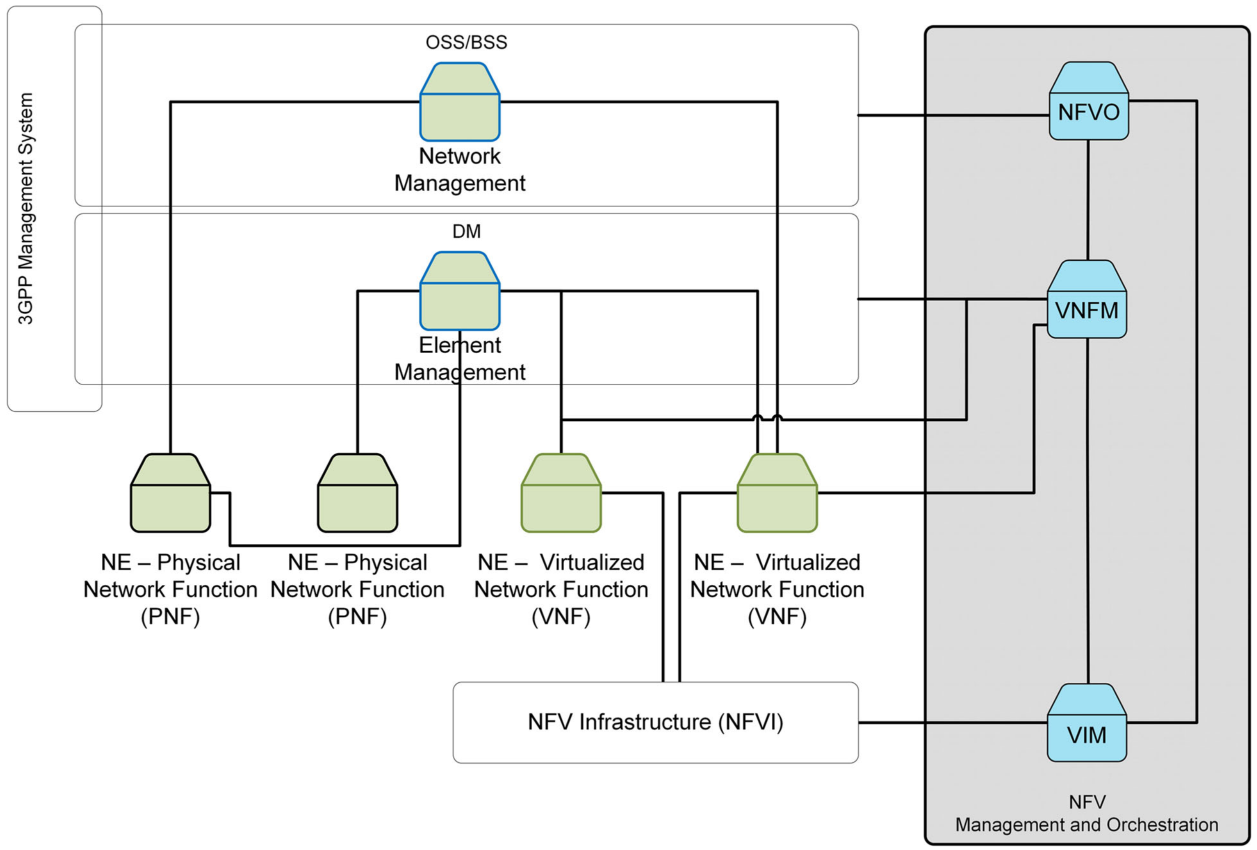

3GPP Management System
OSS/BSS
Network Management
DM
Element Management
NE – Physical Network Function (PNF)
NE – Physical Network Function (PNF)
NE – Virtualized Network Function (VNF)
NE – Virtualized Network Function (VNF)
NFV Infrastructure (NFVI)
NFVO
VNFM
VIM
NFV Management and Orchestration

Fig. 9 Mapping between ETSI NFV-MANO and 3GPP for managing cellular networks. The proposed management and orchestration works for cellular networks with both standard and virtualized network functions

which informs the MME and SMLC of the target identity using the service of interest for investigation. It is worth mentioning that LALS also need to be supported for MEC applications, where the service part of the service-based localization is offered on the local cloud. In this case, the LALS procedure shown in Fig. 6 stays the same; only the SMLC needs to be able to request the service details from the MEC server and include them in the subscriber location report back to the LEA.

3.2 Network Functional Virtualization—NFV

One of the major key technologies that will be integrated in the future 5G systems is virtualization of network functions or NFV. NFV refers to the replacement of traditional specialized hardware devices with software that can be installed on standardized, off-the-shelf hardware [15]. Cellular network operators can use NFV to virtualize the MME or S/P-GW functions to reduce costs and increase flexibility for changes in network capacity, for example. The mapping between the reference ETSI NFV-MANO architecture and 3GPP is shown in Fig. 9. The 3GPP network management comes as a part of the OSS/BSS segment that is controlled by the NFVO. The virtual VNFM manages the 3GPP VNF residing on the NFVI in coordination with the general element management. The element management is also responsible for managing the PNF as part of the 3GPP management system. The NFVI by itself is managed by the VIM.

The introduction of NFV brings several challenges for continuous support of LI and LALS in the current form for conducing cellular network investigations. Because the NFVI can reside in a different jurisdiction than the VNFs, PNFs, and even the NFV-MANO entities, LEAs cannot assume regulated forensic readiness and pre-established points of interception and localization. First, the LEA must ensure that the ADMF and the virtualized interception control elements or the SMLC are trusted and isolated from other VNFs on the same NFVI (which might not be even functions from the same cellular network at all). Second, the ADMF as the LI and LALS root-of-trust needs to interoperate with the other roots-of-trust such as the elements of NFV-MANO. Third, ADMF needs to perform attestation on the VNFs before LI or LALS are invoked to determine whether the target identity is served by VNFs residing in the legally authorized jurisdiction.

For this purpose, [16] discusses potential use of a PKC scheme between the ADMF and the ICEs (as the points of interception), the SMLC, and the NFV-MANO entities. However, LI and LALS can include broad set of services and might be invoked for a longer period of time during which the target identity may start using services from NFVs residing out of the authorized jurisdiction. In this case, the LI and LALS certificates need to be revoked (other alternative is to use shorter expiration times for each certificate but that might result in a PKC management burden). This mechanism has a potential impact on real-time investigations in that critical IRI records or CC data might not be collected while the user and signaling traffic transits through the VNFs due to revoked or expired certificates.

Together with the PKC mechanism, [16] proposes addition of a CCTF to the standard LI architecture to allow for provisioning of CC internal interception functions in a NFV environment. The purpose of the CCTF is to determine the location of the NFV ICE associated to the target CC traffic. In cases where the location and/or addressing information for the ICE is not known until the target identity registers (or makes a call in the case of voice), the IRI typically provides the necessary information for the provisioning of the NFV (e.g., the IP address and port for the content streams). Therefore, in the LI adaptation for NFV shown in Fig. 10, the CCTF is triggered by the IRI intercept function and the ADMF before the LI is provisioned through the CC interception function.

3.3 Network slicing

Network slicing is a feature that allows cellular network operators to create customized network partitions per traffic category, performance, or subscriber type [17]. For example, operators can create a slice for CIoT devices or slices for capacity/coverage on demand. These logical partitions are referred to as NSIs and can contain one or more subnets—NSSI. The NSSIs further contain network functions (which can be virtualized, too) belonging to the core and/or the RAN as shown in Fig. 11. The network slicing concept in Rel. 15 assumes business models where (1) network operators can define flexible relationships with their subscribers or (2) different network operators share portions of the network, e.g., the RAN. In both cases, the network operators manage and orchestrate their core networks and optionally share the management of the radio network with other operators.

In general, the concept of network slicing enables multi-tenancy or vertical markets, and so, in Rel. 16, a new business model is discussed where only part of the network is owned and managed by a network operator, e.g., enabling *private slices* [18]. Four potential management options are considered for this business model:

- A network operator provides the virtual/physical infrastructure and the PNF/VNF; a private third party uses the dedicated functionality provided by the network operator
- A network operator provides the virtual/physical infrastructure and the PNF/VNF; a private third party manages some PNF/VNF via APIs provided by the network operator
- A network operator provides the virtual/physical infrastructure; a private third party provides some PNF/VNF
- A private third party provides some PNF/VNF and manages them

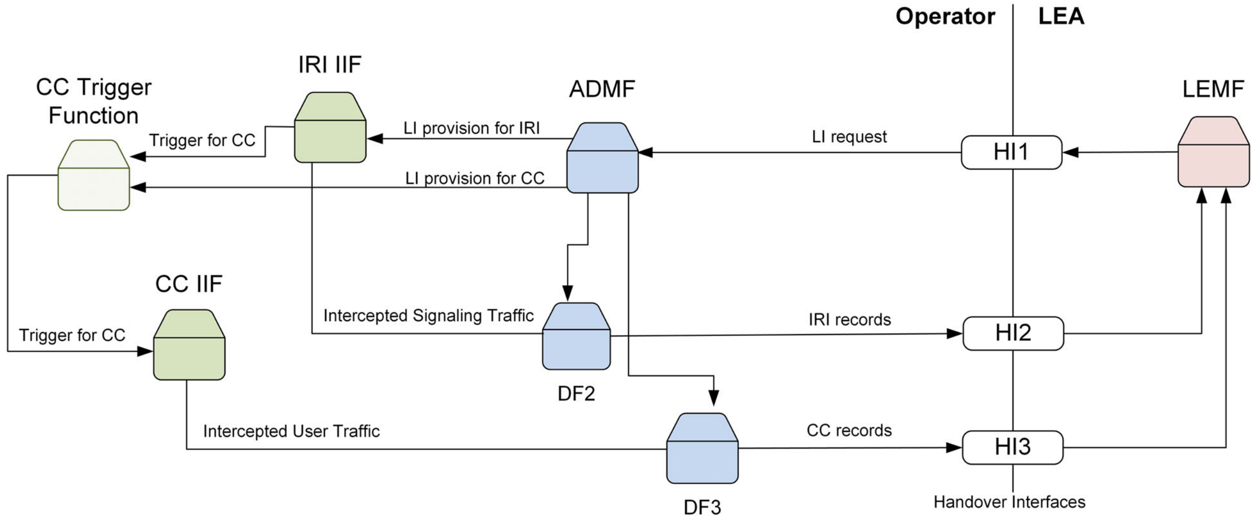


Fig. 10 LI adaptation for networks composed of VNFs. The CCTF is shown as a standalone function but can be implemented as part of the ADMF

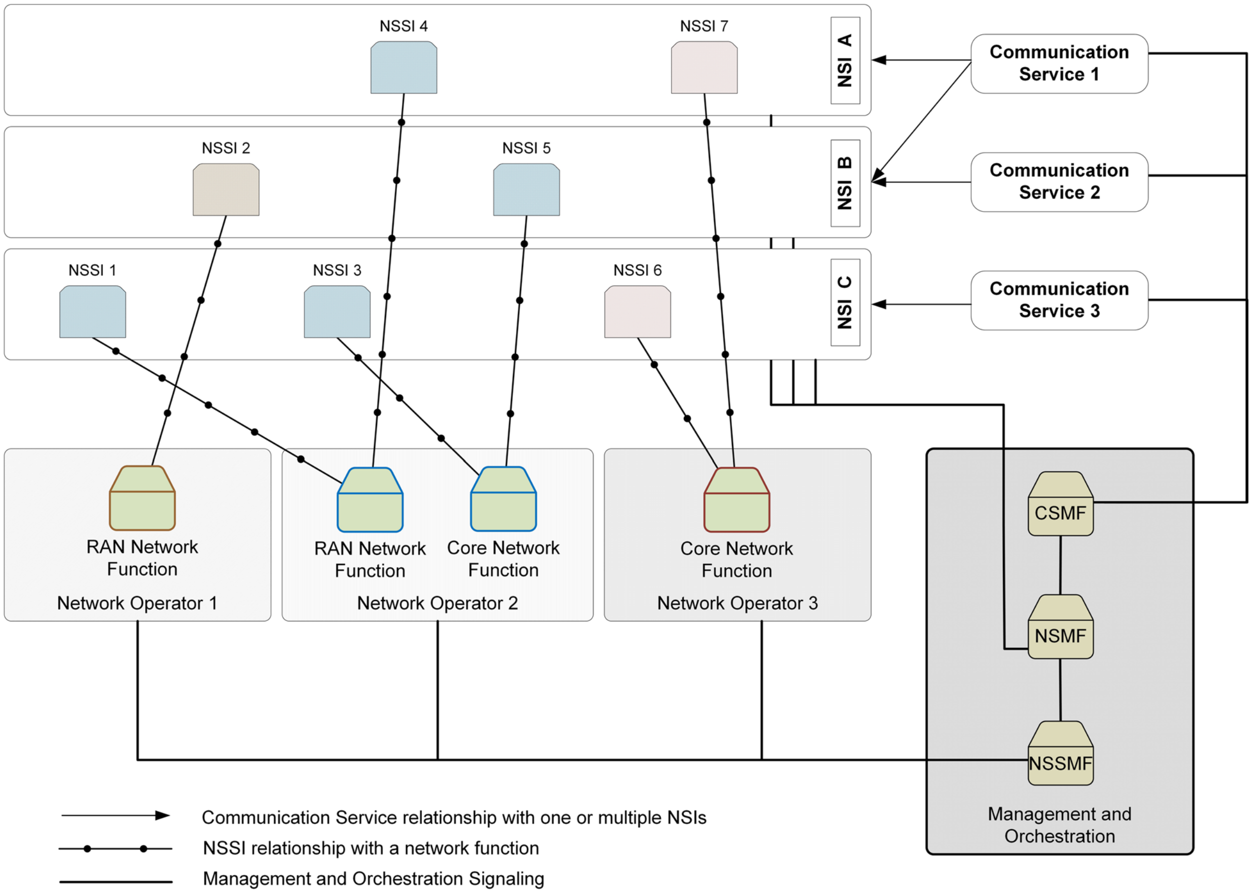


Fig. 11 Rel. 15 network slicing architecture. The CSMF is responsible for translating communication service-related requirement to network slice-related requirements and communicates with the NSMF. The NSMF is responsible for management and orchestration of NSI and communicates with the NSSMF. The NSSMF is responsible for management and orchestration of NSSI

All management options for supporting private slices have an impact on the LI and LALS mechanisms. In the network slicing models from Rel. 15, all the involved operators are subject of national regulation and the exiting LI and LALS mechanisms can be adapted with small modifications as discussed in the next two subsections. However, private third parties might not be regulated, so the forensic investigations of users belonging or using private slices require redefined procedures for LI and LALS. To support LI and LALS for private slices, a trust relationship between the network operators and the private third parties must be defined.

For the first management option, the third party must trust the network operator when provisioning the LI and LALS requests and delivering the cellular network evidence back to the LEA. The third party in this case might need to be allowed to authorize these requests with a direct access to the ADMF. For the second and third second management option, ADMF needs to be adapted so it can provision LI and LALS to the PNF/VNF managed and/or provided by the third party. For the fourth option, the LEA needs to establish separate handover interfaces with the third party. In all cases, the LEA needs to be able to authenticate and verify the trustworthiness of the cellular network evidence delivered by the third party.

3.3.1 *Lawful Interception adaptations for network slicing*

For the Rel. 15 business models, a communication service in a network slicing scenario is a bundle of standard cellular services offered by a communication service provider, like packet data or roaming. Each of these services might be offered and fulfilled by different packet data network functions, e.g., S-GW and P-GW can be from one operator and the serving eNBs from another. The LI function therefore has to be modified to enable investigations with multiple sources of IRI records and CC data for a target identity with a communication service of interest as shown in Fig. 12. The ADMF configures the LI on the CSMF, which identifies the NSI involved and propagates a CMS_ID to the NSMF so the LEA can distinguish between multiple concurrent services used by a target identity in the same time. The NSMF adds the

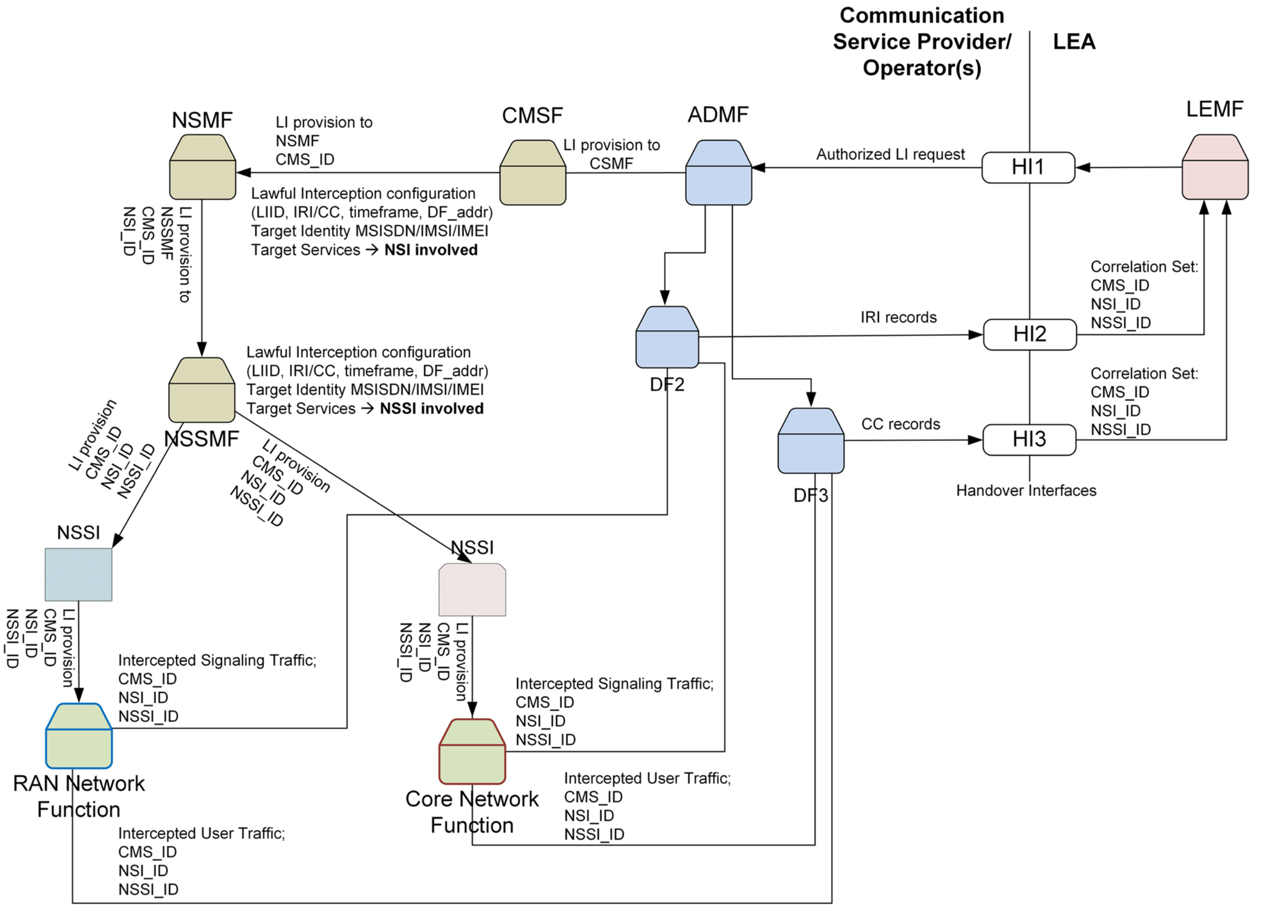

Communication Service Provider/ Operator(s)
LEA
NSMF
LI provision to NSMF CMS_ID
CMSF
LI provision to CSMF
ADMF
Authorized LI request
HI1
LEMF
Lawful Interception configuration (LIID, IRI/CC, timeframe, DF_addr) Target Identity MSISDN/IMSI/IMEI Target Services → NSI involved
LI provision to NSSMF CMS_ID NSI_ID
Correlation Set: CMS_ID NSI_ID NSSI_ID
IRI records
HI2
Lawful Interception configuration (LIID, IRI/CC, timeframe, DF_addr) Target Identity MSISDN/IMSI/IMEI Target Services → NSSI involved
DF2
Correlation Set: CMS_ID NSI_ID NSSI_ID
CC records
HI3
NSSMF
LI provision CMS_ID NSI_ID NSSI_ID
LI provision CMS_ID NSI_ID NSSI_ID
DF3
Handover Interfaces
NSSI
NSSI
LI provision CMS_ID NSI_ID NSSI_ID
LI provision CMS_ID NSI_ID NSSI_ID
Intercepted Signaling Traffic; CMS_ID NSI_ID NSSI_ID
Intercepted Signaling Traffic; CMS_ID NSI_ID NSSI_ID
RAN Network Function
Core Network Function
Intercepted User Traffic; CMS_ID NSI_ID NSSI_ID
Intercepted User Traffic; CMS_ID NSI_ID NSSI_ID

Fig. 12 LI adaptations for the Rel. 15 network slicing architecture. For the LEA to be able to distinguish and correlate CIoT traffic (signaling and both IP and non-IP traffic), a triplet of IDs including the communication service identifier, the NSI identifier, and the NSSI identifier is proposed

NSI_IDs part of the communication service, identifies the NSSI involved, and sends the updated LI provisioning info to the NSSMF. The NSSMF identifies the NSSIs, adds their NSSI_IDs to the LI configuration, and instructs the serving network functions—which ultimately realize the service of interest—to deliver the requested IRI/CC to DF2 and DF3, respectively. For a Rel. 15 network slicing, the correlation set propagated in the IRI and CC records to the LEA includes the triplet CMS_ID, NSI_ID, and NSSI_ID. These adaptations can be kept for Rel. 16, but the ADMF needs to be updated to support authorization of private slices and the LEMF to receive delivery of IRI records and CC data on a separate set of handover interfaces for the same target identity or communication service.

3.3.2 *Lawful Access Location Services adaptations for network slicing*

The Rel. 15 network slicing offers an interesting opportunity for operators to share the LCS function as part of the second business model that allows RAN sharing. This is an optimization for LALS because the LEA in this case needs to work with only one SMLC instead of multiple SMLCs hosted by each network operator. The immediate and periodic positioning will not be affected because they happen regardless of the communication service currently used by the target identity. For the enhanced location for IRI positioning, the localization IRI records need to include the correlation set of CMS_ID, NSI_ID, and NSSI_ID so the geographical movement trajectories over the investigated period can be reconstructed according to the NSI(s) and NSSI(s) involved in the communication service of interest. These adaptations will also work for the first business model and are shown in Fig. 13.

3.4 Cellular Internet of Things—CIoT

CIoT is a network feature preliminary defined in LTE-Advanced to enable access in licensed spectrum for massive number of IoT devices [19]. CIoT can be implemented in three variants: (1) EC-GSM-IoT, (2) eMTC, and (3) NB-IoT. EC-GSM-IoT introduces coverage extension, LTE-grade security, and improved power efficiency for

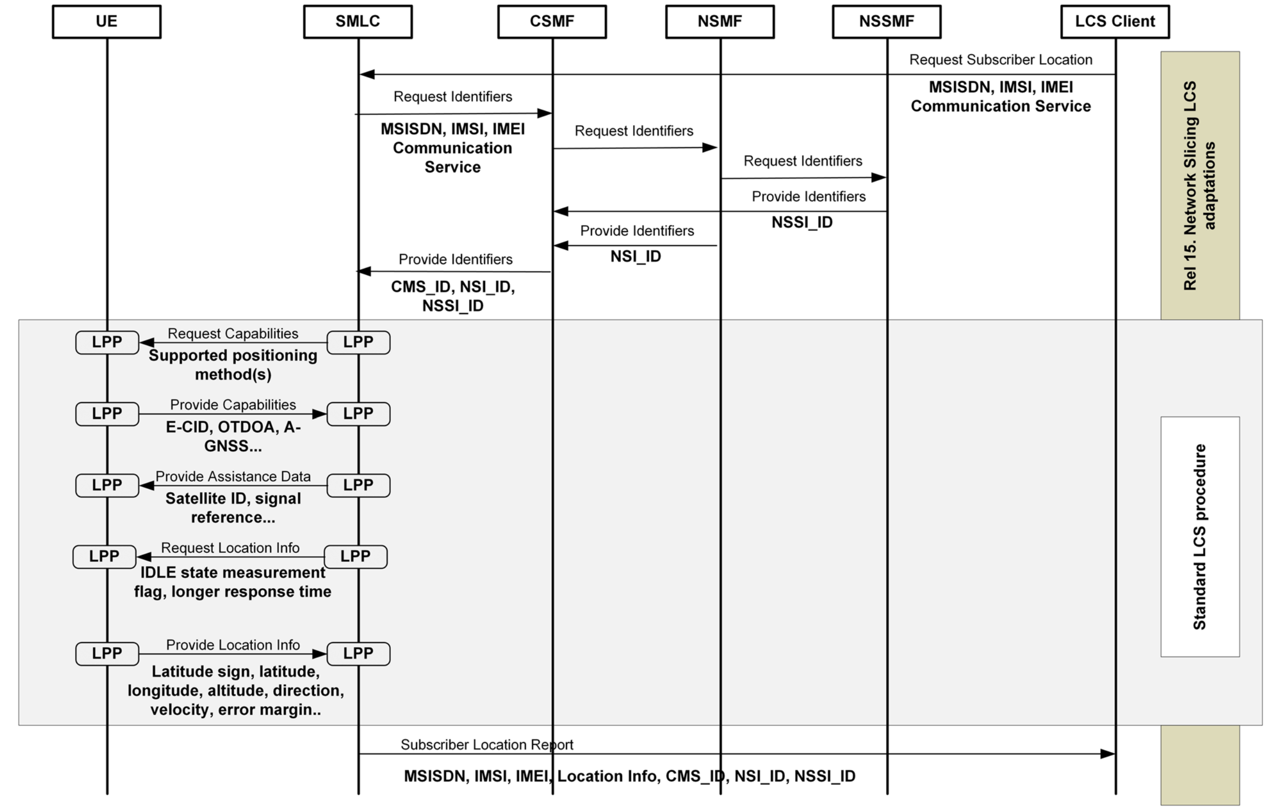

UE
SMLC
CSMF
NSMF
NSSMF
LCS Client
Request Subscriber Location
MSISDN, IMSI, IMEI Communication Service
Request Identifiers
MSISDN, IMSI, IMEI Communication Service
Request Identifiers
Request Identifiers
Provide Identifiers
NSSI_ID
Provide Identifiers
NSI_ID
Provide Identifiers
CMS_ID, NSI_ID, NSSI_ID
Rel 15. Network Slicing LCS adaptations
LPP
Request Capabilities
Supported positioning method(s)
Provide Capabilities
E-CID, OTDOA, A-GNSS...
Provide Assistance Data
Satellite ID, signal reference...
Request Location Info
IDLE state measurement flag, longer response time
Provide Location Info
Latitude sign, latitude, longitude, altitude, direction, velocity, error margin..
Standard LCS procedure
Subscriber Location Report
MSISDN, IMSI, IMEI, Location Info, CMS_ID, NSI_ID, NSSI_ID

Fig. 13 LALS adaptation for the Rel. 15 network slicing architecture. Few extra steps are added in the LCS procedure so the SMLC can include the CMS_ID, NSI_ID, and NSSI_ID in the subscriber location reports sent back to the LEA

legacy machine-to-machine communications. GSM has the largest global coverage footprint and very small time-to-market, which is a huge advantage for readily available CIoT applications [20]. eMTC is an adaptation of the current LTE access to accommodate CIoT applications like wearables, CCTV, object tracking, or smart healthcare. It enables 15-dB enhancement over the standard LTE coverage and extends the DRX to relax the latency and provide bigger delay budget needed for many CIoT applications. eMTC is fully compatible with the standard LTE/LTE-Advanced architecture, making it relatively easy to support in the currently deployed LTE networks [21]. For CIoT applications like smart metering that require modest data rates, relaxed latency, longer battery life, extended coverage, and massive capacity, 3GPP introduces the self-contained NB-IoT radio access. The narrower bandwidth of only 200 kHz allows for significant reduction in device complexity, supporting sporadic (maximum latency of 10 s) and low-rate CIoT traffic (50 kbps) for a battery life between 5 and 10 years [21].

The CIoT network architecture introduces a new node in the EPC, the Cellular IoT Serving Gateway Node (C-SGN), shown in Fig. 14. C-SGN incorporates the MME and S/P-GW roles, performing only necessary functions like simplified NAS signaling, security, and mobility and session management. The C-SGN is fully integrated with the HSS, SMS-GMSC, and IWMSC to enable non-IP services in case the CIoT applications require such.

3.4.1 *Lawful Interception adaptation for CIoT*

The proposed adaptation for support of LI for CIoT devices is shown in Fig. 15. In the CIoT case, the C-SGN accepts the LI requests and configures the ICE depending whether the CIoT user traffic, signalization traffic, or both are needed. C-GSN needs to configure a CIoT identifier so the LEA can distinguish it from IRI records or CC data intercepted for regular (non-CIoT) users. The ADMF can provision this number to C-GSN depending on a local network mapping of specific MSISDN, IMSI, and IMEI numbers specifically dedicated to CIoT devices (operators usually distinguish between different user groups by specific IMSI/MSISDN/IMEI series, but this can cause confusion in cases a user inserts a regular SIM card into a CIoT device. Investigators need to be aware of such anti-forensics actions).

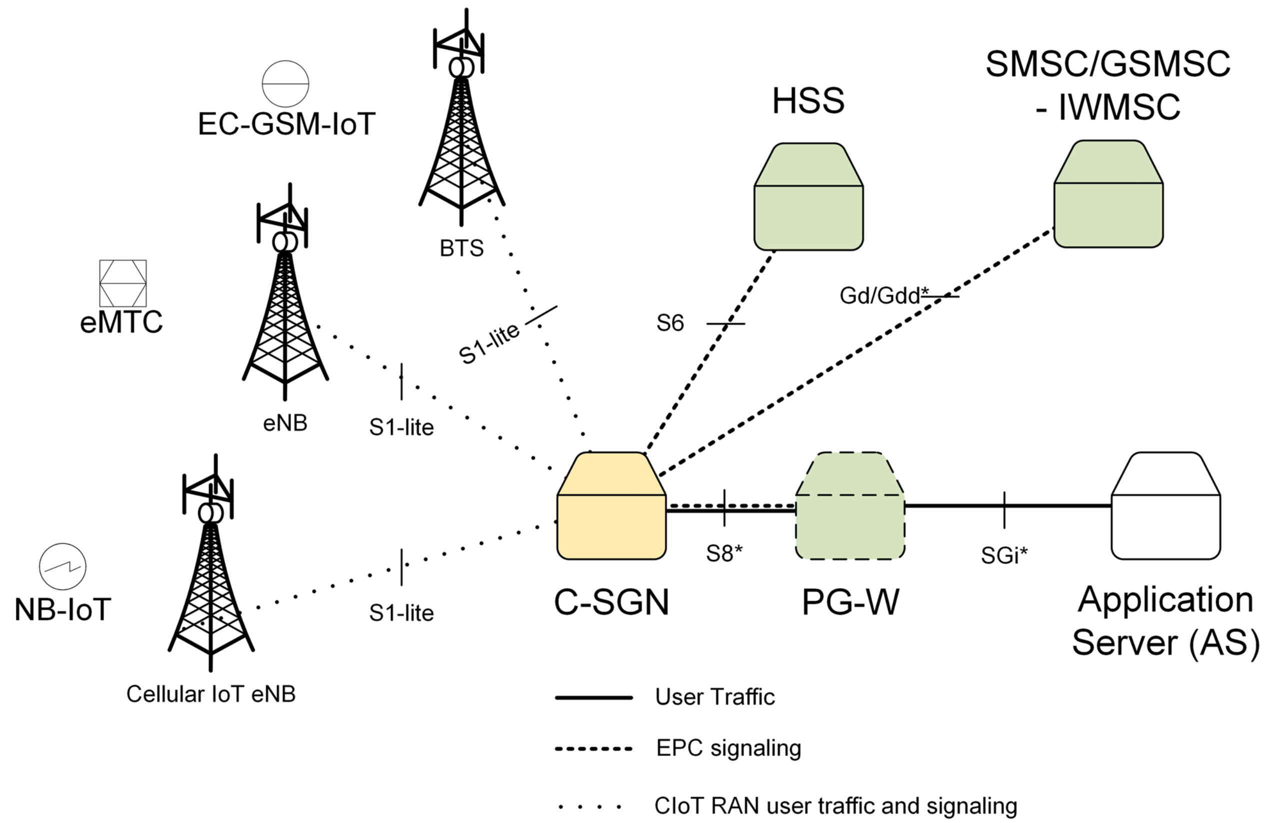


Fig. 14 The general CIoT architecture. The S-GSN communicates user and signaling traffic over the S1-lite interface with the CIoT radio access network. The S8*, SGi*, and Gd/Gdd* interfaces indicate CIoT-specific session management per the IoT application requirements defined in the AS. The application server is realized as a service running on a remote cloud

3.4.2 Lawful Access Location Services adaptation for CIoT

The general LCS architecture for LTE/LTE-Advanced requires adaptations to enable LALS positioning for CIoT devices. The limited computational and memory resources restrict these devices to perform immediate positioning measurements while they are in CONNECTED state, which is a necessary prerequisite for most of the positioning procedures. Therefore, the CIoT devices need to be allowed to perform measurements in IDLE state when they have most of their resources

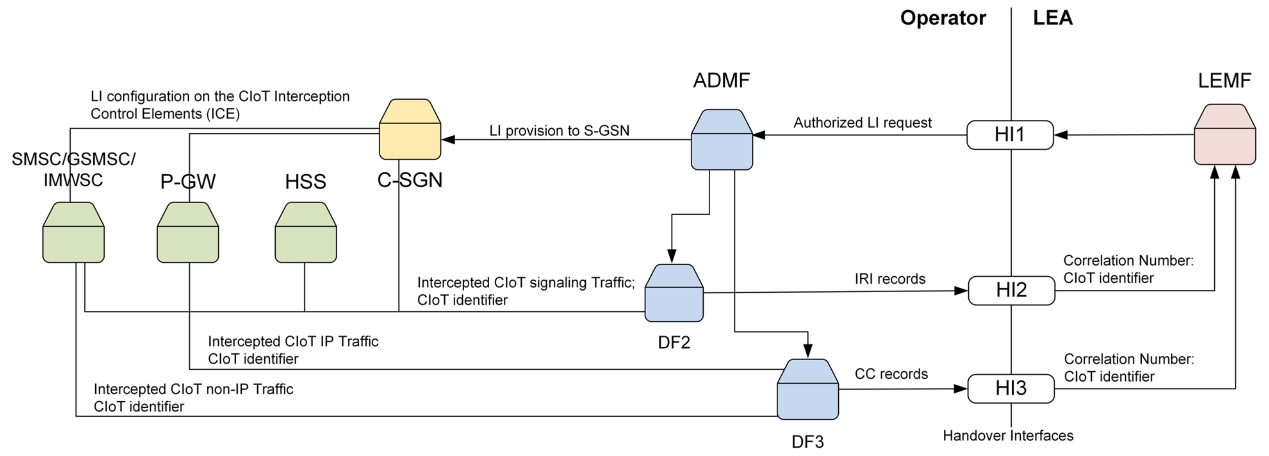

Operator
LEA
ADMF
LEMF
LI configuration on the CIoT Interception Control Elements (ICE)
LI provision to S-GSN
Authorized LI request
HI1
SMSC/GSMSC/ IMWSC
P-GW
HSS
C-SGN
Intercepted CIoT signaling Traffic; CIoT identifier
IRI records
HI2
Correlation Number: CIoT identifier
DF2
Intercepted CIoT IP Traffic CIoT identifier
CC records
HI3
Correlation Number: CIoT identifier
Intercepted CIoT non-IP Traffic CIoT identifier
DF3
Handover Interfaces

Fig. 15 LI integration with the CIoT architecture. For the LEA to be able to distinguish and correlate CIoT traffic (signaling and both IP and non-IP traffic), a CIoT identifier is proposed

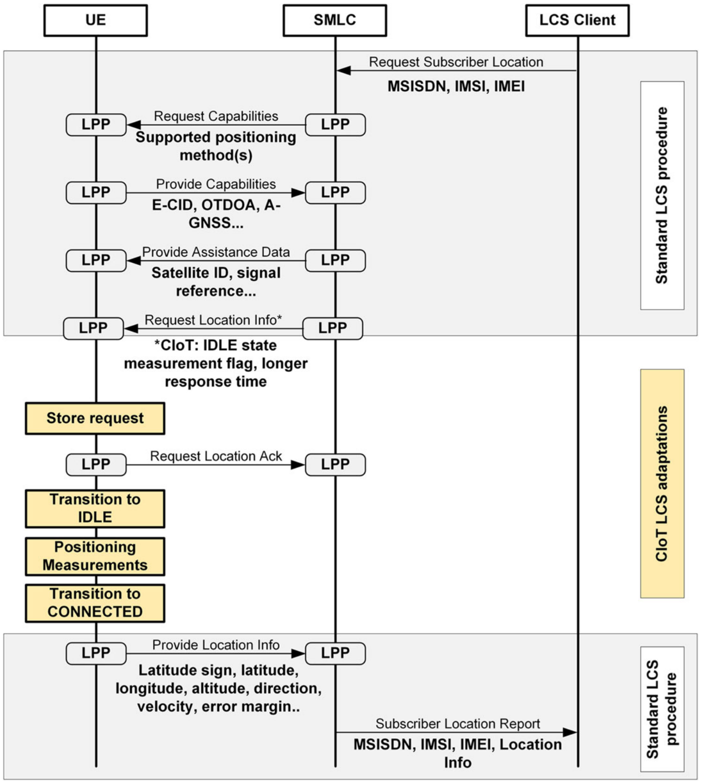


Fig. 16 LALS integration with the CIoT architecture. SMLC must allow for IDLE state measurement for computational and power-restricted CIoT devices

available. In the proposed CIoT LCS procedure shown in Fig. 16, the SMLC uses a flag to indicate support for an IDLE state measurement. In this case, the positioning measurements are performed in IDLE and communicated back in CONNECTED state. The SMLC accommodates this prolongation with an extended timer, depending on the CIoT application [22].

This LCS modification for CIoT affects both the real-time and non-real-time forensic localization. In the case of immediate localization, the LEA has no option but to accommodate to this delay. In the case of periodic localization, the LEA might need to use a larger reporting granularity (fewer reports and a longer report interval) to be able to track the location of a CIoT device over a prolonged period of time. For the enhanced location for IRI localization, the LEA also needs to expect delayed and out-of-order reports, given that many of the target identities will respond to the localization requests in a prolonged and uncoordinated manner.

4 Cellular network forensics—legal and privacy aspects

4.1 Cellular network forensics in the European Union

The use of LI and LALS within the European Union is covered by the Council Resolution 96/C 329/01 requiring the LEA to be able to access all IRI records and CC data from user and signaling traffic transiting or stored by cellular network operators, as well as request subscriber localization information. The 2002/20/EC directive established guidelines concerning cooperation between LEAs and cellular network operators which made LI and LALS a condition for granting cellular networks the authority to operate [23]. The 2002/20/EC directive also contains a number of conditions that may be attached to the general authorization for providing LI and LALS in conformity with Directive 97/66/EC and Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

4.2 Cellular network forensics laws in the USA

In the USA, the CALEA requires that LEAs need to be able to access IRI records and CC data with no degradation and interference to the subscriber service while protecting the privacy and security of subscribers and the respective intercepted material [24]. The Wiretap Act including the Title III of the OCCSSA and the ECPA prohibits unauthorized, nonconsensual interception of wire, oral, or electronic communications by government agencies for target identities that are US citizens. The FISA covers the use of LI and LALS for intelligence purposes where the target identity could not be a US citizen, working as an agent on behalf of a foreign country. The invocation of LI and LALS under FISA requires prior authorization by the FISC federal court. The Title II of US Patriot Act allows LEAs to obtain authorization for LI or LALS by demonstrating that the IRI and CC records are *relevant* for an investigation, rather than the stricter FISA requirement to demonstrate that the target identity is *explicitly* involved in unauthorized activities and terrorism.

4.3 Cooperative cellular network forensic investigations

In general, prior the LI and LALS are invoked, the LEA must obtain a court warrant and implement privacy protections for safe storage and analysis of the acquired cellular network evidence. Warrantless invocation of LI and LALS is possible if it is determined that an emergency situation exists involving immediate danger of death or serious physical injury to any person, conspiratorial activities threatening the national security interest, or conspiratorial activities characteristic of organized crime. The responsible LEA in such a case needs to apply for a warrant approving the interception within few days after the LI and LALS evidence acquisition has occurred to the appropriate court. With a probable increase use of CIoT in the future, however, there is another possibility for another type of warrantless acquisition of cellular network evidence, namely the digital witness methodology proposed in [2] that enables citizens to share their CIoT data with some privacy guarantees.

A CIoT device can be a *digital witness* with the capabilities of identifying, collecting, safeguarding, and communicating cellular network evidence. The digital witness is harmonized with the ISO/IEC 29100 privacy principles to stimulate the cooperation of citizens in forensics investigations. This is an interesting and promising approach for augmenting CIoT LI and LALS; however, the LEA must be able to correlate and possibly verify the evidence material collected from the CIoT digital witnesses with the material acquired from the CIoT network operator.

5 Conclusions

The forensic capabilities of LI and LALS currently available in LTE/LTE-Advanced networks were reviewed to propose adaptations and discuss implementation challenges with the main technologies envisioned for 5G. CUPS, NFV, network slicing, and CIoT are developed largely in insolation so integration into the 5G ecosystem will impact the continuous support for LI and LALS. Different correlation mechanisms per technology, multiple streams of IRI and CC records, and potential inclusion of third parties in the cellular service realization are just some of the challenges LEAs need to address to keep the LI and LALS capabilities in the future 5G networks. Equally relevant is the legal aspect of conducting cellular network investigations. With the traffic served by virtualized functions that can reside in multiple jurisdictions, LEAs also need to find a way to continuously support LI and LALS, especially for real-time investigations. On top of this, LEAs are increasingly challenged with the analysis of third party encrypted CC, which, depending on the jurisdiction, might preclude LEAs to decrypt the user traffic of interest.

Abbreviations

3GPP: 3rd generation partnership project; 5G: 5th generation; A-GNSS: Assisted Global Navigation Satellite Systems; AoA: Angle of Arrival; API: Application programming interface; APN: Access point name; AS: Application server; BSS: Business support systems; C-SGN: Cellular service gateway node; CALEA: Communications Assistance for Law Enforcement Act; CC: Content of Communication; CCTF: CC triggering function; CDR: Charging data records; CGI: Cell global identity; CID: Communication identifier; CIoT: Cellular IoT; CMS: Communication service; CSMF: Communication service management function; CUPS: Control and user plane separation; DNS: Domain name service; DSS: Digital signature standard; E-CGI: Evolved cell global identity; EC-GSM-IoT: Extended coverage for GSM IoT; ECID: Enhanced cell ID; ECPA: Electronic Communications Privacy Act; eDRX: Extended discontinuous reception; eMTC: Evolved machine type communication; EPC-MT-LR: EPC network initiated localization request; EPC-NI-LR: EPC network mobile terminating localization request; EPC: Evolved packet core; ETSI: European telecommunication standardization union; EUTRAN: Evolved UTRAN; FISA: Foreign Intelligence Surveillance Act; FISC: FISA court; GPS: Global positioning system; GSM: Global system for mobile; GTP: Gateway tunneling protocol; HI1: Handover interface 1; HI2: Handover interface 2; HI3: Handover interface 3; HSS: Home subscriber system; HTTPS: HyperText transfer protocol secure; ICE: Interception Control Elements; IMEI: International Mobile Equipment Identity; IMSI: International Mobile Subscriber Identity; IoT: Internet of Things; IP: Internet Protocol; IRI: Interception-Related Information; ISDN: Integrated Service Digital Network; ITOT: ISO Transport Service on top of TCP (ITOT)—also referred to as TPKT; IWMSC: Interconnection Mobile Switching Center; LAC: Location area code; LAI: Location area identity; LALS: Lawful Access Location Services; LCS: Location Services; LEA: Law enforcement agency; LEMF: Law Enforcement Monitoring Facility; LI: Lawful interception; LIID: Lawful interception identifier; LMU: Location measurement units; LPP: LTE positioning protocol; LTE: Long-term evolution; MANO: Management and orchestration; MEC: Mobile edge computing; MME: Mobility management entity; MSC: Mobile switching center; MSISDN: Mobile subscriber ISDN number; NAS: Non-access stratum; NB-IoT: Narrow band IoT; NFV: Network functional virtualization; NFVI: NFV infrastructure; NFVO: NFV orchestrator; NSI: Network slice instance; NSMF: NSI management function; NSSI: Network slice subnet instance; NSSMF: NSSI management function; OAI: Open air interface; OCCSSA: Omnibus Crime Control and Safe Streets Act; OSS: Operations support systems; OTDOA: Observed time difference of arrival; P-GW: Packet gateway; PDCP: Packet data convergence protocol; PFCP: Packet forwarding control protocol; PFD: Packet flow description; PKC: Public key certificate; PLMN: Public land mobile network; PNF: Physical network function; QoS: Quality-of-service; RAN: Radio access network; RSTD: Received signal time difference; RTT: Round-trip time; S-GW: Serving gateway; SIM: Subscriber identity module; SMLC: Service mobile location centers; SMS-GMSC: SMS and gateway MSC; SMS: Short message service; SMSC: SMS center; TAC: Tracking area code; TAI: Tracking area identity; TCP: Transmission control protocol; TDF: Traffic detection function; TOA: Time-of-arrival; TTFF: Time To First Fix; UDP: User datagram protocol; UE: User equipment; UMTS: Universal mobile telecommunication system; UTDOA: Uplink time difference of arrival; UTRAN: UMTS terrestrial radio access network; VIM: Virtual infrastructure manager; VNF: Virtual network function; VNFM: Virtual network function manager

Acknowledgements
The author wishes to acknowledge UTel Systems and ZetX for their technical support and provision of their tools for cellular network forensic analysis.

Availability of data and materials
The materials supporting the conclusions of this article are included within the article.

Authors' contributions
The entire manuscript is a sole contribution of the author. The author read and approved the final manuscript.

Authors' information
Filipo Sharevski received his PhD degree in information security and cyber forensics from Purdue University in 2015. He currently is an assistant professor of cybersecurity at DePaul University, Chicago, IL, USA. He has worked as a cellular network engineer and has conducted practical research in cellular network forensics for his doctoral dissertation. He has established and is currently leading the Cellular Network Security Lab at DePaul University exploring targeted cyberattacks against LTE/LTE-A and future 5G cellular architectures. He has published in internationally recognized and peer-reviewed journals, conferences, and workshops. He is the author of the book "Mobile Network Forensics: Emerging Challenges and Opportunities." His research interests include cellular networks, cyber forensics, cellular Internet of Things, cyberoperations, and cybersecurity gamification.

Competing interests
The author declares that he has no competing interests.

Publisher's Note
Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Received: 15 January 2018 Accepted: 6 June 2018
Published online: 11 July 2018

References
1. Ericsson Mobility Report (2017). https://www.ericsson.com/en/mobility-report. Accessed 12 Oct 2017
2. A Nieto, R Rios, L Javier, IoT-Forensics meets privacy: towards cooperative digital investigations. Sensors. **18**(2), 492 (2018)
3. International Standardization Organization: ISO/IEC 27035:2011 – Information security incident management, (Geneva, 2016). https://www.iso.org/standard/62071.html
4. International Standardization Organization: ISO/IEC 27037:2012 guidelines for identification, collection, acquisition and preservation of digital evidence, (Geneva, 2012). https://www.iso.org/standard/44381.html
5. 3rd Generation Partnership Project: TS 33.106 V14.1.0 - Technical Specification Group Services and System Aspects; 3G security; Lawful interception requirements (Release 14). (3GPP, Sophia Antipolis, 2017). http://www.3gpp.org
6. 3rd Generation Partnership Project: TS 33.108 V14.1.0 - Technical Specification Group Services and System Aspects; 3G security; Handover interface for Lawful Interception (LI) (Release 14). (3GPP, Sophia Antipolis, 2017). http://www.3gpp.org
7. ETS Institute. Lawful Interception (LI); Cloud-Virtual Services for Lawful Interception (LI) and Retained Data (RD). (ETSI, Sophia Antipolis, 2016). http://www.etsi.org/deliver/etsi_tr/101500_101599/101567/01.01.01_60/tr_101567v010101p.pdf. Accessed 20 Jan 2018
8. STINGA Lawful Interception Analyzer. https://utelsystems.com. Accessed 15 Oct 2017
9. ZetX. http://zetx.com. Accessed 15 Oct 2017
10. A Drygajlo, in *Forensic Speaker Recognition: Law Enforcement and Counter Terrorism*, ed. by A Neustein, HA Patil. Automatic speaker recognition for forensic case assessment and interpretation (Springer, New York, 2012), pp. 3–20
11. A Larcher, J-f Bonastre, B Fauve, KA Lee, L Christophe, H Li, JSD Mason, J-y Parfait, in *Interspeech. 14th Annual Conference of the International Speech Communication Association*. ALIZE 3.0—open source toolkit for state-of-the-art speaker recognition, (Lyon, 2013), pp. 2768–2772
12. 3rd Generation Partnership Project: TS 27.071 V14.1.0 - Services and System Aspects; Location Services (LCS); Service description; Stage 1 (Release 14). (3GPP, Sophia Antipolis, 2017)
13. 3rd Generation Partnership Project: TR 38.913 V14.3.0 - Technical Specification Group Radio Access Network; Study on Scenarios and Requirements for Next Generation Access Technologies; (Release 14). (3GPP, Sophia Antipolis, 2017). http://www.3gpp.org
14. P Schmitt, B Landais, FY Yang. Control and user plane separation of EPC nodes (CUPS). (3GPP, Sophia Antipolis). http://www.3gpp.org/cups. Accessed 16 Oct 2017
15. G McQuaid, DR Cione. Lawful interception in virtualized networks. 3GPP, Sophia Antipolis, 2017). https://www.sicurezzaegiustizia.com/lawful-interception-in-virtualized-networks-sept-2017/. Accessed 20 Jan 2018
16. ETS Institute. Network functional virtualization (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications. (ETSI, Sophia Antipolis, 2015). http://www.etsi.org
17. 3rd Generation Partnership Project: TR 28.801 V2.0.1 - Technical Specification Group Services and System Aspects; Telecommunication management; Study on management and orchestration of network slicing for next generation network (Release 15). (3GPP, Sophia Antipolis, 2017). http://www.3gpp.org
18. 3rd Generation Partnership Project: Feasiblity Study on Business Role Models for Network Slicing in Rel. 16. (3GPP, Sophia Antipolis, 2018). http://www.3gpp.org
19. 3rd Generation Partnership Project: 3GPP TR 23.720 V13.0.0 - 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on architecture enhancements for Cellular Internet of Things (Release 13). (3GPP, Sophia Antipolis, 2016). http://www.3gpp.org
20. Cellular networks for massive IoT. https://www.ericsson.com/assets/local/publications/white-papers/wp_iot.pdf. Accessed 14 Oct 2017
21. An overview of 3GPP enhancements on machine to machine communications. IEEE Commun. Mag. **54**(6), 14–21 (2016)
22. 3rd Generation Partnership Project: 3GPP TR 23.730 V14.0.0 - 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on extended architecture support for Cellular Internet of Things (CIoT) (Release 14). (3GPP, Sophia Antipolis, 2016). 3GPP TR 23.730 V14.0.0
23. Government Access to Encrypted Information. https://www.loc.gov/law/help/encrypted-communications/european-union.php. Accessed 17 Oct 2017
24. H Miller, The ready guide for intercept legislation (2007)
25. Open Air Interface. http://www.openairinterface.org. Accessed 6 Jul 2017