Overview of LTE Isolated E-UTRAN Operation for Public Safety

Jad Oueis, Vania Conan, Damien Lavaux, Razvan Stanica, Fabrice Valois

▶ **To cite this version:**

Jad Oueis, Vania Conan, Damien Lavaux, Razvan Stanica, Fabrice Valois. Overview of LTE Isolated E-UTRAN Operation for Public Safety. IEEE Communications Standards Magazine, Institute of Electrical and Electronics Engineers, 2017, 1 (2), pp.98-105. 10.1109/MCOMSTD.2017.1600875 . hal-01573383

HAL Id: hal-01573383

https://hal.archives-ouvertes.fr/hal-01573383

Submitted on 9 Aug 2017

Overview of LTE Isolated E-UTRAN Operation for Public Safety

Jad Oueis[1], Vania Conan[2], Damien Lavaux[2], Razvan Stanica[1], Fabrice Valois[1]

[1] Univ Lyon, INSA Lyon, Inria, CITI, F-69621 Villeurbanne, France
[2] Thales Communications & Security, France

Abstract

In response to the growing demand in the public safety community for broadband communication systems, LTE is currently being adopted as the base technology for next generation public safety networks. In parallel, notable efforts are being made by the 3GPP to enhance the LTE standard in order to offer public safety oriented services. In the recent Release 13, the Isolated E-UTRAN Operation for Public Safety (IOPS) concept was introduced. IOPS aims at maintaining a level of communication between public safety users, offering them local mission-critical services even when the backhaul connectivity to the core network is not fully functional. Isolated operation is usually needed in mission-critical situations, when the infrastructure is damaged or completely destroyed, and in out of coverage areas. In this article, we present a detailed technical overview on the IOPS specifications, and then identify several research prospects and development perspectives opened up by IOPS, being a relatively novel concept in the mobile networks field.

I. Introduction

In the aftermath of a disaster and in emergency situations, first responders, such as law enforcement officers, firefighters and paramedics, are responsible for controlling the situation, and assuring citizens' safety. For their intervention to be efficient, they must be provided with the ability to communicate easily via a reliable, resilient, and secure network. In the past decade, commercial cellular networks witnessed great development, culminating in the 3rd Generation Partnership Program (3GPP) Long-Term Evolution (LTE) technology. Although it still requires further standard enhancements to meet mission critical requirements of first responders, LTE is currently being adopted as the next Public Safety (PS) broadband technology [1].

In many emergency scenarios, both commercial and PS dedicated networks may fail to provide communication for civilians, as well as for PS users. This could happen when the deployed infrastructure is completely destroyed following a disaster, when the deployed Evolved Universal Terrestrial Radio Access Network (E-UTRAN) loses its backhaul connection either completely or partially, or when the network is overloaded due to an increased network demand. Ongoing work by the 3GPP, aiming to adapt LTE to PS use cases, recently tackled this issue by proposing the Isolated E-UTRAN Operation for Public Safety (IOPS) [2].

The first technical specifications of IOPS appeared in 3GPP Release 13 [2-4]. IOPS is an isolated mode of operation that ensures communication between PS users via isolated base stations without backhaul communications. At least local IP connectivity and mission critical voice services are provided to PS users in the absence of a backhaul connection to the core network. IOPS is designed to cope with both infrastructure-less and infrastructure-based scenarios. In case the existing infrastructure was destroyed (e.g. following an earthquake), or initially unavailable (e.g. underground rescue), communication is guaranteed through deployable, easily movable base stations with no backhaul connectivity, that can be installed on the spot. On the other hand, in case the infrastructure remains undamaged, but only the backhaul connectivity is lost or limited (e.g. following a natural disaster), the deployed base stations can still operate by switching to the IOPS mode. In both cases, PS users are provided with coverage and mission-critical services.

IOPS is entering uncharted territory in mobile networks. For years, cellular networks have relied on hierarchical, pre-planned and fixed infrastructure with guaranteed backhaul connectivity. The concept of deployable base stations, such as Home eNodeBs and Relay Nodes, was introduced with small cells, with the main objective of increasing capacity or extending coverage [5]. However, in these cases, backhaul access must be guaranteed, unlike in IOPS.

Being relatively novel and somewhat unknown by the communication community, we introduce in this article the IOPS concept. A detailed overview is given on the technical specifications and requirements of IOPS, as defined by the 3GPP in its latest Release. This article covers the general concept of IOPS, its use cases, the network establishment and configuration specifications, User Equipment (UE) configuration, security considerations, and mobility scenarios in an IOPS network. By reviewing the current status of the standard, we identify open challenges, further pushing for new research prospects and development perspectives in the IOPS standardization.

This work was partially funded by the French Investissement d'Avenir PSPC (Projet Structurant pour la Competitivité) Fed4PMR project.

II. Overview on Public Safety Communication Networks

1) Current Public Safety communication systems

First responders rely on Professional Mobile Radio (PMR)[1] networks for their communications. PMR networks, characterized by their reliability, resiliency, and security, offer a multitude of services designed to meet first responders' mission critical requirements, such as: push-to-talk, group communication, off-network device to device communication, call priority and pre-emption, and end-to-end encryption. However, current PMR networks are based on 2G legacy standards, such as TETRA [6] and P25 [7], mainly offering voice-centric services, with a limited support of data services. Recent enhanced TETRA standards only support data rates in the order of hundreds of kilobits per second [6]. Thus, data-intensive services such as video streaming, image sharing, and online database enquiry, are not supported by current PS systems. Nevertheless, these services can facilitate first responders' interventions, and increase the efficiency of their operations. Unable to provide high bandwidth services, PMR networks are becoming obsolete compared to the rapidly developing LTE commercial networks.

2) LTE for Public Safety

LTE is already adopted as the basis for broadband PS networks in many countries such as the United States[2] and the United Kingdom[3]. The choice of LTE resides in the need to align PS networks with the capabilities of commercial cellular networks. LTE supports high bandwidth, low latency, and high security data services, as well as real-time communication. Moreover, LTE is currently the main wireless technology for broadband communication, with over 300 commercially launched networks globally [8]. Using LTE for PS allows benefiting from this large-scale deployment and the existing ecosystem, in order to reduce Capital Expenditure (CAPEX), i.e. infrastructure costs, as well as Operational Expenditures (OPEX) [8]. Furthermore, as the market for PS systems is much smaller than that of commercial cellular, a significant gap has always existed in the investment and research that goes in PS networks, which contributed in blocking their advancement. By implementing the LTE technical standards, PS operators benefit from the massive innovation ecosystem of these commercial networks. On the other hand, commercial networks also benefit by expanding their markets to include PS agencies. As formulated by Nokia in its call for the European Union to support the migration of European PS networks towards LTE: "a transition to the mobile broadband ecosystem will therefore be performance-enhancing, more efficient, affordable and future-proof" [9].

3) Public safety standardization initiatives in 3GPP

PS communication networks impose stringent requirements in terms of mission critical services, service accessibility, and end-to-end performance [1]. Since Release 11, standardization efforts have been led by 3GPP, in tight cooperation with representatives of the PS community, to adapt LTE to PS requirements. Several PS-oriented specifications have been released, such as:

- Proximity Services (ProSe) (3GPP TS 22.278, Release 12): allows two users in proximity to discover each other and communicate, even when they are out of network coverage.

- Group Communication System Enablers (GCSE) (3GPP TS 22.468, Release 12): provides efficient communication within a group of LTE users. The same content (e.g. voice, video) is provided to multiple users at the same time.

- Mission-Critical Push-To-Talk (MC-PTT) (3GPP TS 22.179, Release 13): users request permission to talk by pressing a button on their device. Only one user is granted the right to talk at a time, while the others listen.

- Isolated E-UTRAN Operation for Public Safety (IOPS) (3GPP TS 22.346, Release 13): enables users to maintain a level of communication in isolated mode without backhaul communication.

Work underway in future releases includes enhancements of the LTE for Public Safety features, along new work items for the SA6 working group, created by the 3GPP for the main purpose of specifying mission-critical applications standards, such as mission critical data and mission critical video.

[1] Also referred to as Land Mobile Radio (LMR).

[2] First Responders Network Authority (FirstNet), USA, http://www.firstnet.gov/about, accessed on 02/2017.

[3] The Emergency Services Network (ESN), UK, http://readyforesn.com/about-esn, accessed on 02/2017.

III. IOPS Standardization

The first IOPS specifications appeared in 3GPP Release 13, frozen in March 2016, as one of the standardization efforts conducted by the 3GPP to enhance LTE to meet PS requirements. The standard includes the general IOPS requirements [2], as well as a description of the architectural concept [3], and security guidelines of IOPS [4].

1) Concept

IOPS allows PS users to maintain a level of communication, providing local IP connectivity and PS services, even without a backhaul link to the traditional core network [2]. A traditional LTE network architecture comprises three main elements: the User Equipment (UE), the E-UTRAN which is the access network, including the base stations referred to as eNodeB, and the Macro Evolved Packet Core (EPC) which is the core network that communicates with packet data networks of the outside world, and handles both data flows and signaling (Fig. 1). An E-UTRAN is referred to as isolated when it loses its backhaul connection to the Macro EPC.

In addition to supporting operation with no backhaul to the Macro EPC, IOPS can take benefit from a limited backhaul connection. Different scenarios were considered in IOPS earlier studies regarding the backhaul state [2]:

- no backhaul: neither the signaling backhaul nor the user data backhaul are available.
- limited bandwidth signaling only backhaul: only a limited bandwidth signaling backhaul is present. Only the signaling of PS user is reliably communicated to the Macro EPC.
- limited bandwidth signaling and user data backhaul: both limited signaling backhaul and limited user data backhaul are present. A limited amount of user data with no guarantee of service could be transmitted.

In Release 13, only the first scenario, in which no backhaul is present, was considered. In the following, we present an overview on the main requirements and guidelines for IOPS in this scenario.

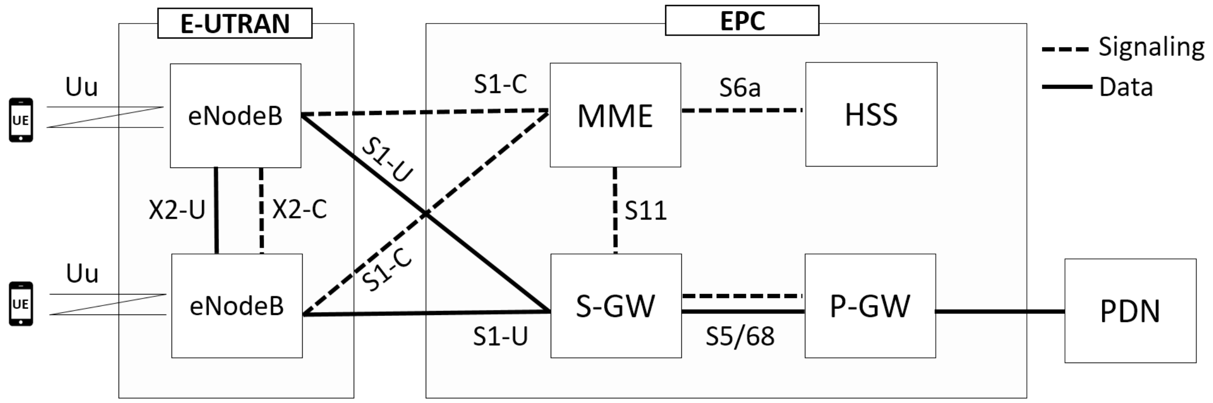


Figure 1 - Standard LTE network architecture. A UE attaches to an eNodeB, which connects to the EPC via backhaul links. The main EPC components are: the Home Subscriber Service (HSS), a central database of network subscribers; the Mobility Management Entity (MME), handling paging, user mobility and authentication, gateway selection, etc.; the Serving Gateway (S-GW) which routes and forwards user data; the Packet Data Network Gateway (P-GW) which communicates with external packet data networks.

2) Local EPC

In order to provide services to PS users without backhaul communication, 3GPP adopted a solution in which IOPS-capable eNodeBs are co-located with, or at least can reach, a Local EPC.

The Local EPC provides the basic functionalities of a traditional Macro EPC [3]. It must at least include the functionalities of the Mobility Management Entity (MME), the Serving Gateway (SGW), the Packet Gateway (PGW), and the Home Subscriber Server (HSS) (Fig 2a). In a Macro EPC, each functionality is usually deployed on a separate dedicated hardware. In a Local EPC, these functionalities can be deployed on the same entity. The Local EPC can be co-located with the eNodeB (Fig 2b, 2d), or deployed as a standalone entity on a separate server (Fig 2c, 2e).

The Local EPC approach considers that an IOPS network comprises [3]:

- a Local EPC and a single IOPS-capable eNodeB, which is co-located (Fig 2b) or has connectivity to the Local EPC (Fig 2c)

- a Local EPC and two or more IOPS-capable eNodeBs, which have connectivity to a single Local EPC (Fig 2d, 2e)

The LTE-Uu radio interface and the Evolved Packet System (EPS) bearer services are supported by the Local EPC. Servers of mission-critical applications can be co-located with the local EPC, in order to provide services over the IOPS network. In case an eNodeB is not co-located with, nor can reach a Local EPC instance, it cannot serve users.

With several eNodeBs co-located with their own Local EPC, it is not necessary to activate all the present EPCs. For example, in Fig 2d, only one Local EPC is activated, to which the other eNodeBs are connected, while the other Local EPCs are not used. Among the problems that arise in this scenario, an important question is the number and the choice of the Local EPCs to be activated. These problems are further discussed in the next section in which we introduce the most prominent IOPS open challenges.

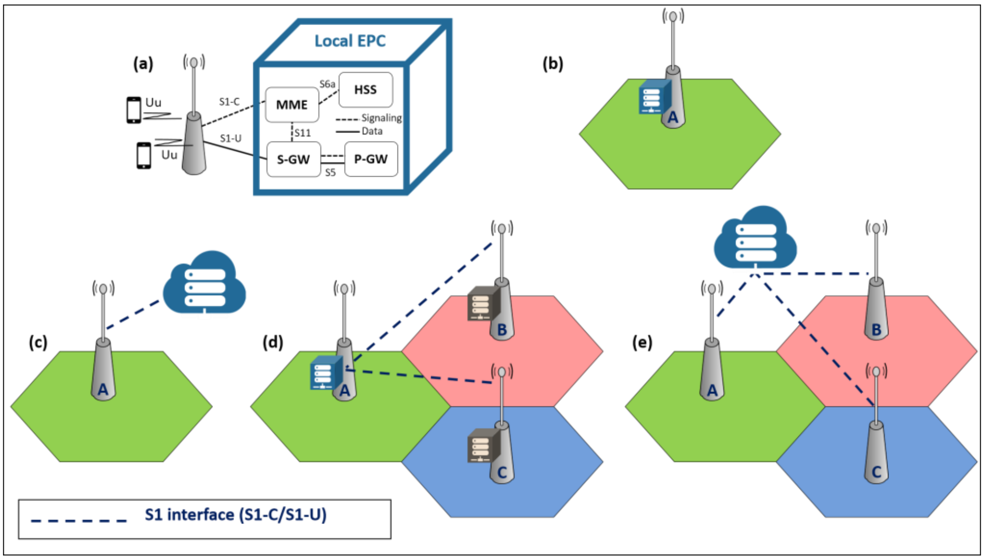


Figure 2 - (a) Local EPC functionalities identical to those of a Macro EPC; (b) An IOPS network comprising a single IOPS-capable eNodeB co-located with a Local EPC; (c) An IOPS network comprising a single IOPS-capable eNodeB which has connectivity to a Local EPC deployed as a standalone entity; (d) An IOPS network comprising multiple IOPS-capable eNodeBs co-located with a Local EPC. In this example, each eNodeB has its own Local EPC. However, only the Local EPC of eNodeB A is activated, and the other eNodeBs connect to it; (e) An IOPS network comprising multiple IOPS-capable eNodeBs which have connectivity to a Local EPC deployed as a standalone entity.

3) IOPS network formation and termination

The IOPS mode of operation without backhaul to a Macro EPC takes place in two situations [2]:

- following a loss of backhaul connectivity to the Macro EPC (e.g. following a natural disaster), the already deployed IOPS-capable eNodeBs enter the IOPS mode of operation. An acceptable level of communication is maintained via an isolated IOPS-capable eNodeB, or a set of connected IOPS-capable eNodeBs (Fig 3a).

- the deployment of one or more nomadic eNodeBs without backhaul to a Macro EPC happens in an isolated location with no infrastructure (e.g. forest fire). The nomadic eNodeBs are IOPS-capable and provide coverage where coverage was not present beforehand (Fig 3b).

In both cases, the fixed and nomadic eNodeBs operate in IOPS mode, without backhaul connectivity, exhibiting similar behaviors[1].

In the case of a fixed eNodeB operating in IOPS mode following backhaul loss, the eNodeB can detect the restoration of the backhaul to the Macro EPC. In this case, connections to the Local EPC are released, the eNodeB stops its IOPS mode of operation and switches back to normal operation.

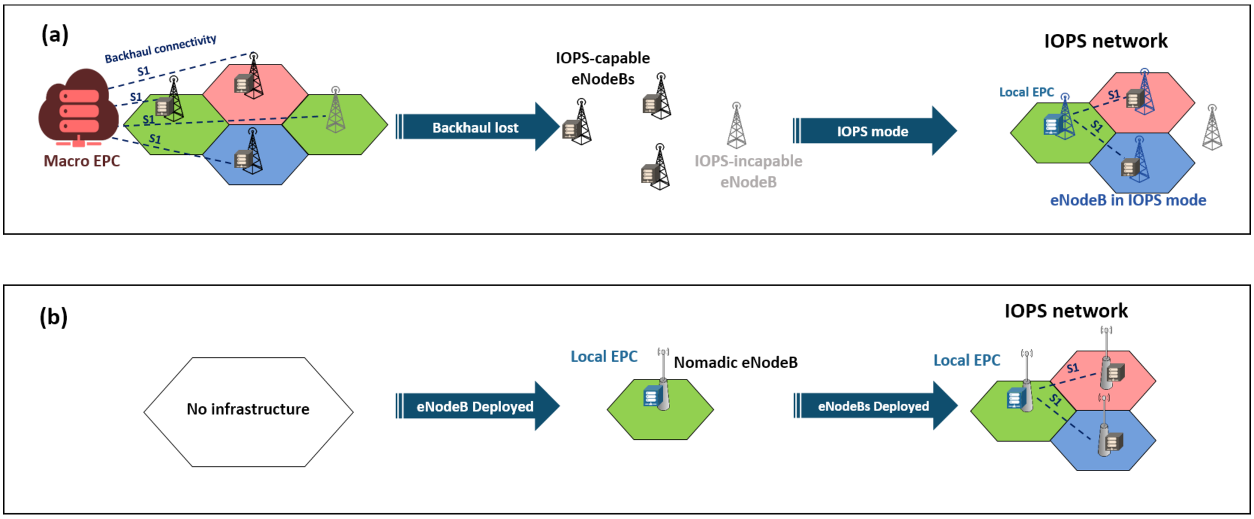


Figure 3 - IOPS network formation: (a) Following the loss of normal backhaul connectivity to the Macro EPC, the already deployed IOPS-capable eNodeBs, co-located with a Local EPC, enter the IOPS mode of operation. The eNodeBs select one Local EPC to connect to, and establish an IOPS network. An IOPS-incapable eNodeB cannot serve users and remains out of service; (b) In an isolated location with no pre-deployed infrastructure, one or more nomadic eNodeBs co-located with a Local EPC are deployed on the spot. When several nomadic eNodeBs are deployed, they can connect to the same Local EPC, and establish an IOPS network.

4) IOPS network configuration

When one or more eNodeBs enter the IOPS mode of operation, they first establish the interface with the MME of the Local EPC. The interface setup between the eNodeB and the MME of the Local EPC follows standard LTE procedures. All IOPS-capable eNodeBs in the IOPS network must be pre-configured with the IP endpoint of the MME of one preferred Local EPC, and optionally, with the IP of one (or more) alternative Local EPC MME(s). The alternative MME will be used if a connection cannot be established with the preferred Local EPC [3].

All Local EPCs deployed by the same operator are considered to be in the same Public Land Mobile Network (PLMN), with the same PLMN-ID, dedicated to IOPS. If a Local EPC is serving one eNodeB, all the cells served by this eNodeB share the same Tracking Area Identity (TAI). If multiple eNodeBs are served by a single Local EPC, configuration of TAIs for IOPS follows local operator policies. However, cells served by eNodeBs connected to different Local EPCs have distinct TAIs in order to trigger a tracking area update upon mobility. A distinction here is made between fixed and nomadic eNodeBs sharing the same PLMN-ID. TAI assigned to cells served by a fixed eNodeB must be different from the TAI of cells of nomadic eNodeBs, since a tracking area update must be triggered between these systems [3].

[1] In the following, unless stated explicitly, no difference is made between the operation of fixed and nomadic eNodeBs.

5) UE configuration

In order to access the IOPS network, the standard proposes a double Universal Subscriber Identity Module (USIM) application solution. An authorized UE must have the IOPS dedicated PLMN-ID configured in a separate USIM application, exclusively for IOPS. For the same UE, the PLMN-ID used to access the normal network is contained in another USIM application. A UE with both USIM applications can display information on the available PLMNs to the end user.

When in IOPS mode, an eNodeB broadcasts its cells as “Not Barred” and “Reserved for Operator Use”. Thus, only authorized UEs, with the IOPS dedicated USIM application, can access the IOPS network, while other users in the same area are barred.

When the UE detects the broadcasted IOPS PLMN-ID in the cell, if no normal PLMN-ID is also detected, the USIM application switches automatically to IOPS mode. However, if a normal PLMN-ID is also detected, it would have a higher priority than the IOPS PLMN-ID. Hence, when both PLMNs are available, the normal one would be chosen with precedence. However, a user can manually switch the USIM application if both were available [3].

When the USIM application is switched, the UE attaches to the local EPC according to standard LTE attachment procedures. Once authenticated, the UE obtains a local IP address and can access local PS services [3].

6) Security

Similarly to LTE standard procedures, when operating in IOPS mode, the Authentication and Key Agreement (AKA) procedure is performed between the USIM application dedicated for IOPS operation, present in IOPS-enabled UEs, and the Local HSS of the Local EPC. The security credentials used by the USIM application dedicated for IOPS are distinct from those used for normal operation (Fig 4). These credentials are configured a priori in the dedicated USIM application, and in all Local HSSs within the Local EPCs [4].

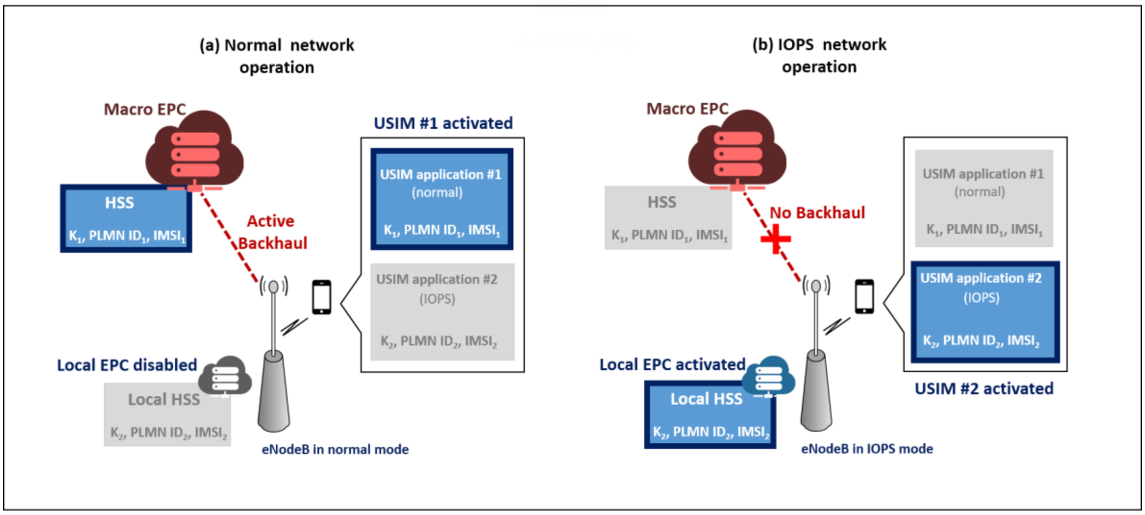

(a) Normal network operation
Macro EPC
HSS
K_1, PLMN ID_1, $IMSI_1$
Active Backhaul
USIM #1 activated
USIM application #1 (normal)
K_1, PLMN ID_1, $IMSI_1$
USIM application #2 (IOPS)
K_2, PLMN ID_2, $IMSI_2$
Local EPC disabled
Local HSS
K_2, PLMN ID_2, $IMSI_2$
eNodeB in normal mode
(b) IOPS network operation
Macro EPC
HSS
K_1, PLMN ID_1, $IMSI_1$
No Backhaul
USIM application #1 (normal)
K_1, PLMN ID_1, $IMSI_1$
USIM application #2 (IOPS)
K_2, PLMN ID_2, $IMSI_2$
USIM #2 activated
Local EPC activated
Local HSS
K_2, PLMN ID_2, $IMSI_2$
eNodeB in IOPS mode

Figure 4 - (a) Normal network operation: UE’s USIM application #1 for normal operation is activated, while USIM application #2 dedicated for IOPS is deactivated. USIM application #1 contains the set of security credentials also configured in the HSS of the Macro EPC for UE authentication; (b) IOPS network operation: UE’s USIM application #2 dedicated for IOPS is activated following backhaul connection loss. The Local EPC is activated, and the Local HSS, pre-configured with the dedicated set of credentials, is used for authentication.

7) Mobility

Multiple UE mobility scenarios are possible in an IOPS network (Fig 5) [3]:

- UE transitions from a cell controlled by the Macro EPC to a cell operating in IOPS mode.
- UE transitions from a cell operating in IOPS mode to a cell controlled by the Macro EPC.
- Inter-IOPS network cell transition: UE transitions from a cell operating in IOPS mode whose eNodeB is served by one Local EPC to a cell also operating in IOPS mode whose eNodeB is served by a different Local EPC.
- Intra-IOPS network cell transition: UE transitions between cells operating in IOPS mode whose eNodeB(s) are served by the same Local EPC.

In the first two cases, the UE switches from normal mode to IOPS mode and vice versa. The UE must switch the USIM application, and then initiate the attach procedure towards the new target EPC. The last two cases follow normal EPC mobility management procedures, since there is no change in the PLMN-ID. The third case is analogous to inter-MME handover in standard LTE procedures, since the UE changes cells but also changes its serving MME. The fourth case is analogous to an intra-MME handover since the UE remains associated with the same MME, in the same Local EPC.

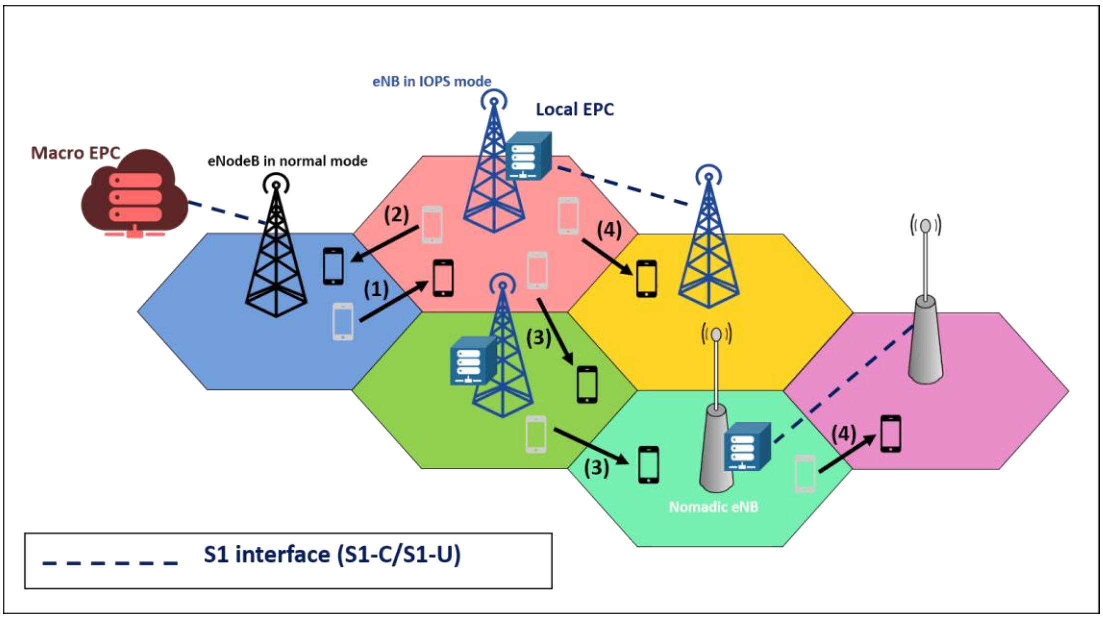


Figure 5 - Handover scenarios in an IOPS network: (1) UE transitions from a cell served by the Macro EPC to a cell operating in IOPS mode served by Local EPC; (2) UE transitions from a cell operating in IOPS mode to a cell served by the Macro EPC; (3) UE transitions between IOPS cells from a cell whose eNodeB is served by one Local EPC to a cell whose eNodeB is served by a different Local EPC; (4) UE transitions between IOPS cells whose eNodeBs are served by the same Local EPC.

IV. IOPS Challenges

The novel concept of isolated base stations, featured in IOPS, opens up numerous research perspectives, as further enhancements are needed to complete the IOPS standardization. IOPS networks should be provisioned to support mission-critical services, which are mostly real-time services imposing stringent performance requirements, as well as a sufficient number of PS users, depending on the scale of the emergency in question. In the following, we briefly discuss some of the challenges that lie ahead towards the full development of reliable IOPS networks.

1) Limited backhaul scenarios

Limited backhaul scenarios occur, for example, when a natural or a man-made disaster partially destroys the existing communication infrastructure, and IOPS networks are installed to this impacted region. A limited backhaul can be used for signaling between an E-UTRAN site and other nearby infrastructures to provide local services. Novel solutions limiting the signaling exchanges must be developed in order to comply with the limited backhaul, which is not sufficient for normal operation. In this case, the need for a local EPC is to be studied. Work underway in Release 14 tackles scenarios in which the backhaul exists, but suffers from a limited bandwidth [10].

2) Inter-eNodeB wireless connectivity

Studying inter-eNodeB wireless connectivity is relevant when several eNodeBs are deployed to cover a wider area. In order to provide services, all the eNodeBs in the IOPS network must be able to reach the Local EPC. This implies the need for inter-eNodeB connectivity.

No standardized solutions exist today to provide LTE in-band inter-eNodeB connectivity. The only known connectivity between two neighboring eNodeBs is provided by the X2 interface. Nevertheless, X2 is only used for handover purposes, and interference coordination. Using X2 to route data and signaling traffic between eNodeBs and towards a local EPC is not yet standardized.

To address this issue, LTE in-band solutions allowing inter-eNodeB connectivity were proposed. Apostolaras et al. [11] proposed connecting neighboring eNodeBs via enhanced UEs capable of associating with multiple eNodeBs. A UE associated simultaneously to two eNodeBs can forward traffic between them. However, this solution requires new types of UEs, and a high UE density in the network. On the other hand, Favraud et al. [12] introduced an enhanced eNodeB design (e2NB), consisting of a physical eNodeB co-located with a Local EPC, and extended with several UE stacks. By depicting the behavior of a physical UE, the UE stack allows the e2NB to discover neighboring e2NBs and attach to one of them via standard UE attachment procedures, establishing an in-band inter-eNodeB link. Nevertheless, the two e2NBs must be at proximity for the attachment to take place, restricting this approach to close by eNodeBs. In this case, questions are raised on the resulting interference between the e2NBs.

3) Local EPC dimensioning problem

The IOPS standard recommends choosing one preferred Local EPC to which all eNodeBs must connect. All data and signaling traffic is transferred through the Local EPC. This raises questions on the capacity of a single Local EPC to handle this amount of traffic, and provide the necessary services to all users. The mission critical nature of IOPS networks impose stringent requirements in terms of end-to-end delay, quality of service (QoS), and resiliency. Eventually, a single Local EPC might be insufficient to serve an IOPS network while respecting these requirements, and multiple Local EPCs should be activated. In this case, performance thresholds must be set in order to determine the number of Local EPCs needed in a network. This number depends on the above constraints, and more particularly on the number of deployed eNodeBs, as well as the number of users in the network.

However, having multiple Local EPCs in what is supposed to be a single IOPS network may not be always practical. Let us suppose that two eNodeBs are each served by a different Local EPC. If two users, each attached to one of those eNodeBs, need to communicate via a communication service, passing through two different Local EPCs further complicates the communication process, in comparison to one Local EPC serving both users. Moreover, two eNodeBs served by different Local EPCs are each connected to different MMEs. This triggers inter-MME handover upon user mobility, creating additional signaling overhead in the network. Determining the number of Local EPCs in an IOPS network is still an open challenge, where inter-EPC and intra-EPC signaling costs must be considered.

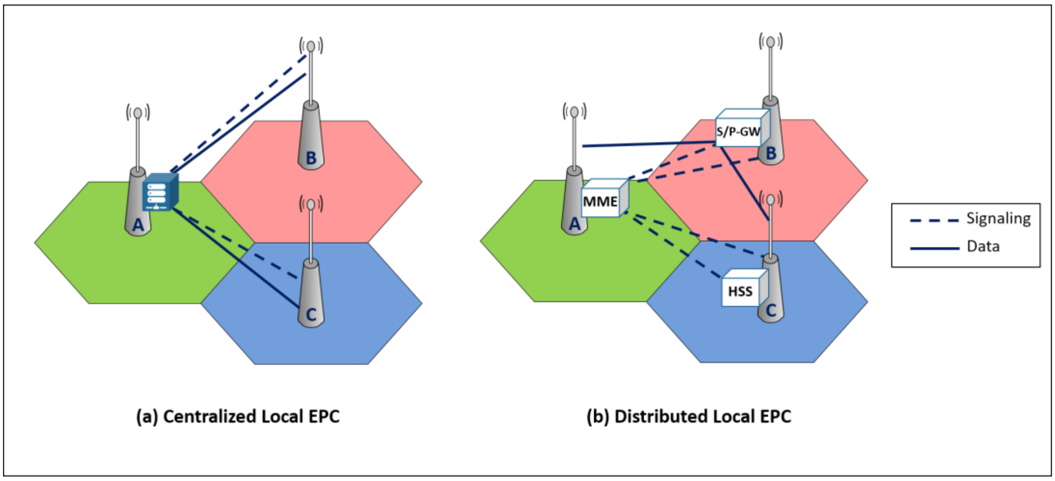
4) Local EPC placement problem

Multiple Local EPCs can exist in the network. For example, several eNodeBs can be co-located with their own Local EPC, or multiple Local EPC servers can be present. After answering the question on how many Local EPCs must be activated in the network, a major question is raised: which one(s) of the present Local EPCs must be activated? The answer to this question is not always evident, since multiple factors must be taken into consideration in selecting which Local EPC to activate.

All the eNodeBs in the network have a certain amount of traffic to route towards the Local EPC to which they are connected (and vice-versa). This traffic is routed either directly, if the Local EPC is at one hop, or through the interconnected eNodeBs in a multi-hop fashion. Consequently, determining the EPC placement must take into consideration the links between the eNodeBs, their capacity, and their quality in order to ensure that a given amount of signaling and data traffic can circulate in the network. Moreover, the Local EPC placement must take into consideration the tight performance requirements of a PS network in terms of QoS and end-to-end delay.

5) Splitting and distributing Local EPC functions

The concept of a Local EPC co-located with an eNodeB opens up new perspectives on having a distributed EPC rather than a centralized one. Indeed, it is possible to deploy on each eNodeB one of the EPC functionalities instead of having all of them co-located with a single eNodeB (Fig 6). The benefits of such an approach is the load balancing it achieves by mitigating the signaling traffic destined to or originated from the activated Local EPC of the selected eNodeB. Nevertheless, in a centralized approach, all the entities are on the same node, meaning all the EPC internal signaling traffic (i.e. between EPC components) does not consume bandwidth on the links between the eNodeBs. On the other hand, in a distributed approach, while congestion may be relaxed on a particular eNodeB, the EPC internal signaling traffic is routed through the links between the eNodeBs, limiting their capacities. The trade-offs between both approaches must be further studied. In the same context, EPC distribution is among the 3GPP work items for Release 14 [13], in which the separation of user plane and control plane functionalities of the EPC is considered.



(a) Centralized Local EPC

(b) Distributed Local EPC

Figure 6 - (a) Centralized Local EPC: all the functionalities of the Local EPC are co-located with eNodeB A; (b) Distributed Local EPC: The functionalities of the Local EPC are distributed respectively among the three eNodeBs.

6) Network dynamicity

In its current stages, IOPS operation only considers fixed E-UTRAN. However, IOPS is mainly developed for PS mission critical situations, where dynamicity in the network seems inevitable: new eNodeBs can be added, turned off or even moved. In the same context, moving cells are currently gaining momentum (e.g. convoys), especially in mission critical scenarios [14]. Network dynamicity leads to topology changes, directly affecting the network configuration and connectivity. Changes in the topology, as well as high mobility can cause established links to the EPC to drop, creating network coverage problems. Since service disruption is not tolerated in such situations, the disconnected eNodeB must react rapidly in order to discover another Local EPC to connect to, or even activate its own Local EPC to re-establish access to the network. In the case of a single activated Local EPC in the network, changing topologies can affect the choice of the selected Local EPC, where a previously selected Local EPC may not be suitable for the new topology anymore. In this case, adaptation to the new topology must be triggered. The tight performance requirements must be respected at all times throughout the deployment and network configuration changes.

7) Radio resource control

Many challenges lie ahead regarding radio resource control in the IOPS context. A first step in the configuration of the nomadic eNodeBs is a spectral analysis allowing to detect for each eNodeB the occupied resources already in use in their vicinity, and those available. eNodeBs should then decide which ones to use. Classification of free resources and selection criteria must be carefully studied. With multiple interconnected eNodeBs, interference is an issue not to be neglected. Interference management should be considered to ensure that the eNodeBs are robust despite being in an environment with aggressive interference. Indeed, reliable and resilient communication must be guaranteed between the deployed eNodeBs on one hand, and between the eNodeB and the users on the other. This further requires efficient radio resources utilization strategies.

V. Conclusion

In recent years, we witnessed a growing demand for advanced data-centric PS networks, surpassing the outdated voice-centric technologies of the past. With LTE chosen as the base technology for future PS networks, a first step was to fill the gap between PS mission critical requirements and LTE features. Remarkable efforts have been made by the 3GPP in standardizing LTE PS-oriented services. Recently, the IOPS feature was proposed, aiming at providing communication services to PS users when their backhaul is not fully functional. The isolated mode of operation usually occurs following disasters, completely destroying or damaging the infrastructure, and in out of coverage areas. In this article, we described the first technical details of the IOPS feature, standardized in Release 13 on top of LTE. Then, building on its shortcomings, we discussed future perspectives to evolve IOPS. Seeing the novelty of the IOPS concept in the mobile networks field, several research opportunities open up, from which we identify for example inter-eNodeB wireless backhauling, Local EPC dimensioning, placement and distribution problems. Likewise, many research perspectives lie ahead for other LTE for Public Safety features. Cooperation between researchers, PS community, and 3GPP is of key importance to move forward towards an effective PS communication system for first responders.

References:

[1] T. Doumi et al., “LTE for PS Networks”, *IEEE Commun. Mag.*, Vol. 51, no. 2, Feb. 2013, pp. 106-112.

[2] 3GPP TS 22.346, “Technical Specification Group Services and System Aspects; Isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Stage 1 (Release 13).”, Sept. 2014.

[3] 3GPP TR 23.797, “Technical Specification Group Services and System Aspects; Study on architecture enhancements to support isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety (Release 13)”, June 2015.

[4] 3GPP TR 33.897, “Technical Specification Group Services and System Aspects; Study on isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety; Security aspects (Release 13), Mar. 2016.

[5] T. Nakamura et al., “Trends in small cell enhancements in LTE advanced”, *IEEE Commun. Mag.*, Vol. 51, no. 2, Feb. 2013, pp. 98-105.

[6] ETSI TR 102 580 V1.1.1, “Terrestrial Trunked Radio (TETRA), Release 2”, Oct. 2007.

[7] Codan Radio Communications, “P25 Radio Systems Training Guide”, Sept. 2013, available at https://www.codanradio.com/wp-content/uploads/TG-001-4-0-0-P25-Training-Guide.pdf, accessed on 02/2017.

[8] R. Liebhart et al., *LTE for Public Safety*, John Wiley & Sons, 2015.

[9] NOKIA, “PS Services enhanced by LTE Networks”, Nov. 2015, available at http://networks.nokia.com/file/47326/nokia-government-relations-public-safety-services-enhanced-by-lte-networks, accessed on 02/2017.

[10] 3GPP TR 23.798, “Technical Specification Group Services and System Aspects; Study on Isolated E-

UTRAN Operation for Public Safety; Enhancements (Release 14)”, May 2016.

[11] A. Apostolaras et al., “Evolved User Equipment for Collaborative Wireless Backhauling in Next Generation Cellular Networks”, *Proc. IEEE SECON*, June 2015, pp. 408-416.

[12] R. Favraud and N. Nikaein, “Wireless Mesh Backhauling for LTE/LTE-A Networks”, *Proc. IEEE MILCOM*, Oct. 2015, pp. 695-700.

[13] 3GPP TR 23.714, “Technical Specification Group Services and System Aspects; Study on control and user plane separation of EPC nodes (Release 14)”, June 2016.

[14] R. Favraud et al., "Toward moving PS networks", *IEEE Commun. Mag.*, Vol. 54, no. 3, Mar. 2016, pp. 14-20.

Biographies:

JAD OUEIS (jad.oueis@insa-lyon.fr) is pursuing a Ph.D. degree in telecommunications and networking at INSA Lyon, France. He is a member of the Inria AGORA team at the CITI laboratory. He received an M.S. degree in computer science, focused on networking, from INSA Lyon, in 2015, and an Engineering degree in telecommunication from the Lebanese University, Lebanon, in 2015. His current research interests include mobile network architectures and autonomous organization of professional mobile radio (PMR) networks.

VANIA CONAN (vania.conan@thalesgroup.com) is a senior research expert in networking and communications at Thales Communications & Security (TCS), in Gennevilliers, France. He received an Engineering degree (1990), Ph.D. in computer science (1996) from Mines ParisTech, an Habilitation degree from Université Pierre et Marie Curie, Paris (2012). He is presently head of the networking laboratory in the Advanced Studies department at TCS. In the past years he has been conducting research in the field of wireless & ad-hoc networking, including cross-layer, opportunistic protocols and network coding. He has published over 60 international conference and journal papers and filed several patents in networking technologies. His current research topics include cross-layer design of mobile network protocols and virtualized network design.

DAMIEN LAVAUX (damien.lavaux@thalesgroup.com) is an advanced studies Engineer at Thales Communications & Security, France. He received his Engineering degree from ESME-Sudria Paris engineering school specialized in Telecommunications Networks in 2006. He has been involved in research projects since 2007, and his current research topics cover wireless, mobile and ad hoc networks, from software and IP protocol perspective, with a focus on mission-critical communications. He coordinated the awarded FP-7 HIT-GATE European project, was technical manager of PPDR-TC, and recently participated in numbers of European project including 5G-ENSURE, FP7-CONECT, FP7-COGEU, and FP7-MOTO.

RAZVAN STANICA [M] (razvan.stanica@insa-lyon.fr) is an Associate Professor with the Telecommunications department at INSA Lyon and member of the Inria AGORA team at the CITI laboratory, since 2012. He received Ph.D. and M.Eng. degrees in telecommunications and networking from INP Toulouse, in 2011 and 2008, respectively. He also holds a M.Eng. degree from the University Politehnica of Bucharest (Romania). His current research covers the subjects of mobile data analytics, mobile network architectures and data collection in IoT networks.

FABRICE VALOIS (fabrice.valois@insa-lyon.fr) is a full professor at INSA Lyon (France) since 2008. Previously, he was associate professor at the same place. He is also the head of the CITI research lab, Lyon, France. His research interests are focused on wireless and cellular networking, including self-organization protocols, 4G/5G networks, data-aggregation in WSN, networks for IoT. He has published more than 90 journal and conference papers. He received his M.S. degree in Computer Science, in 1996, and his Ph.D. in Computer Science, in 2000, from the University of Versailles.