SDN for Public Safety Networks

Michelle Wetterwald, Damien Saucez, Xuan-Nam Nguyen, Thierry Turletti

▶ **To cite this version:**

Michelle Wetterwald, Damien Saucez, Xuan-Nam Nguyen, Thierry Turletti. SDN for Public Safety Networks. [Research Report] Inria Sophia Antipolis. 2016. hal-01400746

HAL Id: hal-01400746
https://inria.hal.science/hal-01400746

Submitted on 22 Nov 2016

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

SDN for Public Safety Networks

Michelle Wetterwald*, Damien Saucez†, Xuan-Nam Nguyen†, Thierry Turletti†
∗ Université Côte d'Azur, Inria, France
† HeNetBot, France

March 1, 2016

Abstract

Commercial users of modern communications networks have benefited from a huge progress of the related technologies. However, Public Safety Networks (PSNs) and devices did not follow the same trend. Very often, they still rely on voice or low speed data communications, tempting first responders to use their own private devices when they need to exchange real-time video or geolocation information. Under this consideration, national authorities and specialized organizations have recently initiated the integration of more recent technologies, such as cellular Long Term Evolution (LTE), even though they need further developments to cope with the harsh usages that safety personnel may face. This report proposes to move the evolution of these networks towards the recent evolution of networking technologies started with Software Defined networking (SDN) and Network Functions Virtualization (NFV). Based on the requirements derived from a standardized earthquake scenario and a study of the main improvements brought by this network softwarization, it analyzes how SDN and NFV can solve part of the issues raised with commercial LTE and enhance PSN communications. The capabilities of these new technologies are applied to a list of characteristics required by mission-critical networks, e.g., rapid deployment, reliability, security or resilience, taking advantage of features such as the separation between control and data planes or the simplified dynamic resources management. The resulting enhancements are then illustrated using example frameworks published in the literature for Cloud Radio Access Networks, resilient backhaul solution, isolated base stations, SDN-based architecture or Service Function Chaining.

1 Introduction

Mobile communications and the Internet have revolutionized our ways of life. They have even merged together with the introduction of the smartphone, which delivers performances at an order of magnitude beyond comparison with the first personal computers sold on the market. Computing and digital technologies now

progress at an meteoric rate towards higher data speed, larger bandwidth, seamless mobility or the Internet of Things (IoT). All these new features mandate improved characteristics of mobile networks, including enhanced flexibility, security or scalability. A recent and growing trend in network management and control aims at meeting these new requirements by the introduction of Software Defined Network (SDN) and Network Function Virtualization (NFV) technologies. Their objective is to bring to the networks the software flexibility and scalability that will allow them to better fulfill the upcoming needs of network operators and their users.

However, some of the mobile communications users that would most need these new technologies still stay behind, namely the Public Safety Networks (PSNs) users. When the LTE and 4G deployment base grows at a fast pace, PSN users still depend on 2G data communications, when not restricted to voice. Until recently, the digitalization of their Professional Mobile Radio (PMR) was led by a few major projects such as Terrestrial Trunked Radio (TETRA) or Project 25 [6]. TETRA has been deployed in Europe, Middle East, Asia and Latin America since 1995. It provides mostly voice and dispatch services to mobile terminals operating in direct mode (DMO), trunk mode (TMO) through a dedicated infrastructure, or by using neighbour terminals as relays. Data services are also available, but at very low speed, from 80 kbps up to potentially 500 kbps [11], using TETRA Release 2 also known as TETRA Enhanced Data Service (TEDS). The wide geographical coverage enabled by the usage of low frequency bands permits one to deploy an infrastructure with a reduced number of base stations. On its side, the collaborative Project 25, or P25, standardizes an equivalent system for Land Mobile Radio (LMR), mainly deployed in Northern America, Australia and New Zealand. The latest version defines data services at a low level of data rates similar to TEDS.

PSNs carry a mission critical objective, with human lives depending on the successful exchange of information such as devices location, dispatch services or alert messages. Fire brigades or police departments are organized in highly mobile groups of individuals respecting a strong hierarchical configuration, which necessitates different levels of priorities and end-to-end security. They may work in very harsh environments such as earthquake destruction, fires or flooding and are expected to provide relief under any circumstances and in any location. Beyond the voice and specific services that they receive from their rugged mobile devices, PSN users tend to start taking advantage of more evolved and powerful applications, such as real-time video, temperature or heart-rate sensing from their private commercial smartphones.

Under the consideration that even teenagers own a device much more powerful than first responders, several countries and specialized organizations have launched the definition or funding of the evolution of the PSN. Their objective is to integrate the latest advances of mobile communications and offer technologies at a level equivalent to public commercial networks to their users. In the UK, the Emergency Service Network (ESN) will start its deployment in 2016, targeting police, firefighters and ambulances [19]. In the US, the FirstNet authority [10] plans the establishment of one single inter-operable, highly reliable and resilient

wireless broadband network to serve police, firefighters, paramedics, and command centers. The TETRA and Critical Communications Association (TCCA) has recently selected LTE (Long Term Evolution) as the technology to complement TETRA for broadband communications. Enhancements to LTE and LTE-Advanced (LTE-A) have been designed and standardized under Release 12 of the 3GPP, as described in [6] to cope with the additional features necessary to support the PSN operations, such as those described in Section 2.1. At the same time, various new technologies aiming to enhance the performance and efficiency of digital communication networks have sprung up in the past years. Software Defined Networking (SDN) is presented in Section 2.2. It introduces a clear decomposition of control and data plane, which permits one to perform the forwarding at flow level according to fine-grained rules. This section also introduces Network Function Virtualisation (NFV) and Service Function Chaining that complement SDN by adding further flexibility and increasing scalability. Hence it is a natural tendency to propose the benefits of these new technologies to the design of future PSNs, as shown in Section 3. In Section 3.1, we analyze what are the features required for the PSN scenarios. Section 3.2 presents the C-RAN technology, which introduces flexibility on the fronthaul network. A set of solutions based on virtualization is sketched in Section 3.3. They address the resiliency of the backhaul network and enable the operation of isolated cells. In Section 3.4, SDN-based frameworks are presented, where the dynamic management of flows enables improved flexibility for the PSN services. Finally, Section 4 concludes this study.

2 Background

2.1 Public Safety Networks

2.1.1 An emergency scenario: the earthquake

Public Safety (PS) agencies must accommodate a very large range of events, which can be classified into two categories. A first category of events requires mainly prevention. The PS users must ensure the safety of the community during big events like sports or festivals. A main characteristic of this category of events is that it is usually planned well in advance and the technical staffs have sufficient time to anticipate and extend, or re-organize the communication network as required by the event. The second category of events requires healing to respond and restore a viable situation after a natural disaster or a criminal event has occurred. Earthquakes, major storms, bombing and mass transport accidents fall into this category. Contrary to the first category, the latter events are unplanned. They may even witness the destruction of the existing infrastructure, drastically reducing the means of communications for first responders and for the public citizens in general, at a time when they have to deal with emergency requirements.

A typical event of the second category is the earthquake, which scenario has been described in [8] and is pictured in Figure 1. In order to remain as

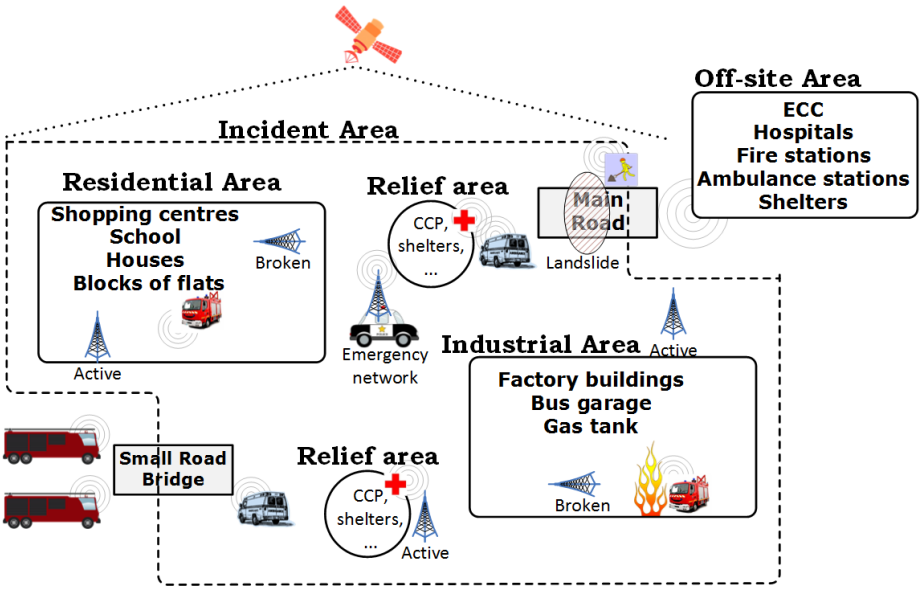

Figure 1: Illustration of the earthquake scenario.

comprehensive as possible, this scenario pictures the event in two sub-areas, a residential neighbourhood and an industrial estate. The residential neighbourhood is composed of apartment buildings as well as individual houses, schools and stores including a petrol station. The earthquake brings down the school and a few other buildings, starts a fire in one of the shops in the commercial center, threatening to spread to other stores and, even worse, to the petrol station. A lot of people get trapped under the buildings, in varying conditions, while others who could escape run away from the danger into the streets. Globally, a large part of the buildings show a high risk of collapsing. The telecommunications network is partly destroyed, creating large coverage holes in the area. The industrial estate contains mainly factory buildings hosting a large number of employees, a bus garage and a gas tank. The area can be accessed only through two roads, one large and a second narrow one spanning a river on a small old bridge. Here as well, the shock brings down the factory buildings, trapping the employees inside. Moreover, it sets a fire in the bus garage, triggers a landslide that closes the main access road and breaks the utility infrastructure for water, electricity and telecommunications. Some cracks can be observed on the small old bridge, which restricts the access through the narrow road only to light vehicles.

Very rapidly, the emergency call centers receive a large number of messages requesting help and inform the first-aid teams and local authorities. The event brings into the affected area an increasing number of actors. In the first minutes after the quake strikes, firefighters, Search and Rescue (SAR) teams, medical services and police units arrive on scene to secure the hazard area, i.e., the area

that was most struck and where individuals may be endangered, as well as a larger and safer zone around it, where most of the first responder teams can be installed, the incident area. They prevent unauthorized access and start their relief operation. An emergency Casualty Collection Point (CCP) is established to receive and triage the victims according to their condition. Rapidly, the whole site gets organized under the governance of a hierarchical management structure of Emergency Control Centers (ECC) receiving instructions and reporting to an off-site Local Emergency Management Authority (LEMA). Other off-site services, e.g., ambulance stations, fire stations, hospitals, shelters such as sports hall belonging to local authorities call up their staff for on-site or remote assistance. The different teams are dispatched in the incident and the hazard areas by their relevant ECC. Relief locations, with temporary shelters and medical equipment are settled in the incident area to receive the victims, care for them according to their conditions and bring them suitably out of the incident area, where they will be further treated or released. Until the last patient has been helped, the SAR teams keep moving between the hazard areas and the relief locations. Additional firefighter teams try to reach the scene, but their big trucks are blocked at the obstructed accesses, delaying the resolution of the fires. Technical experts start assessing the level of the damages to the infrastructure. Road department experts evaluate the stability of the old bridge, exchanging pictures with remote engineers. Construction companies begin evacuation of the mud on the main access road to restore the vehicle traffic flow, assisted by defense forces, under the remote and local direction of geologists. Power, water and food supply are gradually restored by local utility companies and authorities. Repair teams start installing an emergency communication network to compensate for the destroyed infrastructure, after which they tackle the restoration of the original telecommunications networks.

All along, lightly affected and off-site citizens try to contact their relatives to learn whether they have been affected or not, have been moved to hospitals, to shelters or to other places. The media try to exchange information with their headquarters, sending reports for the news magazines and TV shows. Both types of users can only rely on the possible usage of the remnants of the telecommunications infrastructure that are still available, and as soon as they are operational, on the authorized parts of the restored networks.

2.1.2 Requirements

The scenario presented in the previous paragraph, which shows a worst case event, allows deriving the main requirements for future PSNs.

In a first step, it shows the large diversity of actors and other citizens that have to be accommodated by the networks, as well as their needs. Today, the existing PS communications rely mainly on voice conversations, but real-time pictures, video, access to databases, geolocation, purpose-made PS applications could highly improve the impact and efficiency of the rescue missions. Secondly, the scenario also demonstrates that the different groups require different types of communications. The rescue personnel is linked through group communica-

tions to their teammates and dispatching commandments, because they keep sharing real-time information. In existing networks, they use a push-to-talk broadcast mechanism, providing mainly group voice communications. Only one device transmits at one time and all the others listen, based on priority, e.g., the dispatcher's device has a higher priority. The devices are hardened against external conditions, such as high temperature, and are very easy to use, even with heavy protective gloves [11], which are not part of the common features of commercial smartphones. The PS communications must be restricted to a specific geographical area, covering the hazard area where the teams operate. From the ECC point of view, reporting upwards in the hierarchy or requesting information from the local control center rather requires one-to-one communications. These communications must be granted a high priority level in the network, either by owning a guaranteed and private spectrum, or by enforcing QoS mechanisms that increase their priority compared to commercial users in the case where the network is shared. Even more, emergency PS users ought to have higher priority than regular PS users.

[19] gives the different levels of deployment options for future PSNs, especially when taking into account the sharing of the mobile broadband (MBB) network. It ranges from a separate private PSN, to RAN sharing, to considering the PSN as a prioritized virtual operator network or as an overlay over the commercial MBB network. It also considers the possibility for the PS devices to roam to any available MBB network, while operating at a higher priority level when this is made relevant due to external conditions. Roaming also allows to benefit from heterogeneous services such as Wi-Fi or satellite access when they are available, either because they were not destroyed or because they could be established as a temporary emergency solution. The cost for such solutions varies in a wide range. Using a dedicated allocated frequency spectrum with specific devices does not allow taking advantage of scalability savings, as could be the case with devices operating in commercial frequency bands. The network deployment must be flexible enough to easily accommodate any or a mix of the previous options.

These deployment options introduce three major requirements on future PSNs: (1) full geographical coverage, potentially through heterogeneous accesses; (2) robustness and reliability of the network to avoid losing the connection at a critical time; and (3) resilience provided by pooling, back-up connections, traffic load balancing or automated management tools. The full coverage and the resilience may also be achieved using technologies that allow deploying rapidly extensions to the existing and still usable infrastructure, e.g. by pre-installed cells in emergency vehicles. When the full coverage is not feasible because of the failing infrastructure, the mobile devices must be able to interact directly with one another or to serve as relays or gateways to neighbour devices. This is known as Device-to-Device (D2D) communications. With the objective to guarantee communications between the incident area and the off-site locations, the PSN must take into account the large geographical distribution of devices and external server locations. Accordingly, the network planning must be flexible and scalable to accommodate a rapid increase of the number of PS

actors brought on-site in the incident area and able to cope with the high mobility of teams such as SAR, which permanently move back and forth between the hazard area and the ECC, or of the ambulances that transport casualties to the off-site hospitals.

The security of the network, from a physical or cyber point of view, is of extreme importance. Network peripherals and data centers must not be brought down easily after their installation. Capability to access the network must be restricted both at device and at user level. All the traffic must be protected, whether it relates to the management, control or user plane of communications. The confidentiality of each transaction and conversation must be preserved, either inside each team or between a local ECC and the off-site LEMA, with the possibility to separate the different PS teams and agencies inside the PSN.

2.2 Network Softwarization

Networks today became so complex that it was necessary to rethink the way they were conceived to provide higher level of abstraction to increase their efficiency (e.g., cost, energy) and simplify their management. To that aim, *Software-Defined Networking* (SDN) [20, 25, 16] has been proposed. SDN advocates a clear separation between the data-plane, composed of the various forwarding devices, and the control-plane implementing the network control logic. This principle of separation is not so novel but was hardly reachable so-far because of technical limitations. However, nowadays with the generalization of virtualization and the potentially high performance that can be reached by commodity hardware, it is possible to implement efficiently the separation between the control and the data planes.

The general idea of SDN is illustrated in Fig. 2. The separation between the control and the data planes is realized by a *Southbound API* while the network logic is implemented by a logically centralized *Controller Platform* to which network applications interact by the means of a *Northbound API*. The controller platform manages the state of forwarding elements (e.g., switches and routers) directly with the southbound interface. This approach reduces the complexity of forwarding elements as their only role is to forward data packets in the network.

OpenFlow [18] is by far the most mature implementation of the southbound interface [20, 25, 16, 14, 15]. Interestingly, OpenFlow started in the academia but rapidly received much attention from the industry such that nowadays, all major vendors support OpenFlow in their commercial products [20]. The project became so important that the *Open Network Foundation* (ONF) [12] driven by the most influential actors of the Internet (e.g., Google, Facebook, Microsoft, Cisco) has been created to design, improve, and maintain the OpenFlow protocol and its satellite components.

While usually forwarding decisions are taken on a per destination basis, in OpenFlow all forwarding decisions are performed on a flow basis. This approach permits a fine-grain granularity in the way traffic is managed within the network. An OpenFlow switch consists of flow tables, each containing a prioritized

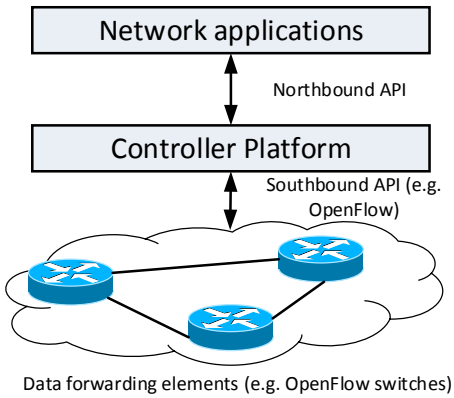

Figure 2: Generic architecture of a SDN network.

list of rules that determine how packets have to be processed by the switch. Conceptually, a rule is composed of three components: a matching pattern, an actions field, and counters. The matching pattern forms a predicate whose value is computed on-the-fly by the switch based on packet meta-information (e.g., source IP address, destination port, VLAN tag). All packets making true the matching pattern predicate are said to belong to the same flow. The actions specified in the actions field of the rule are applied to every packet of the corresponding flow. The most common actions are: forwarding, dropping, or rewriting the packets. Finally, the counters are used to keep statistics on the flows. As a packet may match multiple matching patterns, each rule is associated with a priority and only the rule with the highest priority that matches the packet is considered to take actions on it. The prioritization of rules permits constructing multiple levels of granularity. Fig. 3 summarizes the architecture of OpenFlow and the interactions between the various network components.

In operation, when an OpenFlow switch receives a packet, it checks its flow tables. If the packet matches no rule, the switch may send a request to the controller to determine what actions to perform on the packet. The switch then stores the information so it can process packets accordingly for any further packet belonging to the same flow as the initial packet.

SDN allows to separate data-plane and control-plane components by the means of abstractions such as OpenFlow. However, with the generalization of software solutions in networking, it is possible to complement this abstraction with the virtualization of the network functions themselves. This approach known as *Network Function Virtualization* or *NFV* relies on the fact that network functions can be implemented in software and thus be virtualized and operated on commercial off-the-shelf (COTS) machines. A direct benefit of this approach is in the costs reduction. However, as functions are virtualized and run on virtual machines, it also results in more flexibility and scalability as virtual

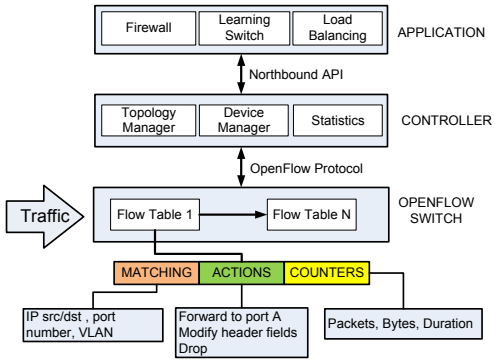

Figure 3: OpenFlow architecture.

machines can be migrated at anytime or hardware can be upgraded without interrupting operations. When network functions are virtualized and SDN is used, then *Service Function Chaining (SFC)* is straightforward. SFC consists in linking network functions to produce services. As every component is software and virtualized, service chains can be modified at anytime to provide new services or to adapt to the load.

3 How can SDN and NFV improve PSN communications

3.1 Required features for PSN scenarios

By their very nature, Public Safety Networks are challenging as they are supposed to work properly even in chaotic situations such that priority management, fault tolerance, and rapidity of deployment are the key features to implement in order to build PSN solutions. The generalization of the software approach in networking with SDN, NFV, and SFC permits to design the new generation of PSNs in an elegant way and sections below show examples of solutions leveraging it. OpenFlow is a key technology to enable efficient priority management. Indeed, in OpenFlow network decisions are decided on a flow basis, for arbitrary flow definition, and implemented in the form of rules with priority levels. It thus means that flows can be treated differently based on policies implemented by the controller and as the controller has a full view of the network, it ensures the strict respect of the policies. The centralization of decisions may appear as a weakness of SDN. However, the centralization of decisions avoids transient situations where all network components try to converge to a new stable state thanks to distributed algorithms, it thus avoids inconsistencies and potential transient loops. The centralization also simplifies fault diagnosis and recovery. In addition, with the virtualization of network functions, it is

straightforward to migrate network functions on different pieces of hardware in case of fault of the underlay. Nevertheless to benefit from all that, it is necessary to build logically centralized control planes that keep the good centralization properties without impairing the robustness of the entire system, as shown in the sections that follow. Finally, the usage of virtual functions and SDN allows rapid deployment of PSNs as functions can be configured and updated on the fly without any particular intervention on the device itself.

3.2 Cloud Radio Access Networks (C-RAN)

In current mobile communication networks, Baseband units (BBUs) are usually co-located with the cell towers on-site. They run on proprietary hardware and are designed for worst-case peak loads. However, through NFV, BBUs can be virtualized and run on general purpose computers. Such centralized virtual BBUs clusters can be provisioned on demand and represent a good replacement for on-site installations of BBUs in distributed geographical locations. This new mobile network architecture, called Cloud[1] Radio Access Network (C-RAN), can bring many advantages in a PSN context. The first, an antenna-integrated Remote Radio Head (RRH) is easy to deploy close to an affected area. Second, a higher system capacity and lower power consumption can be achieved when installing RRHs close to the rescue teams since the wireless signal will propagate on a short distance to reach them. Third, smart cooperative multiple-radio resource management can be used (and higher bandwidth) as the baseband processing is centralized in a data center (BBU pool), as shown in Figure 4.

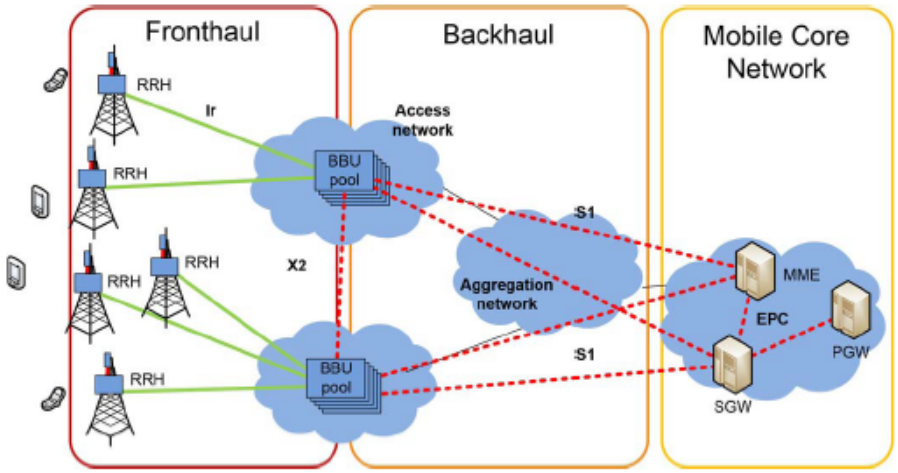

Figure 4: CRAN Architecture. Source:[4]

[1] C-RAN also refers to Centralized-, Cooperative- or Clean- RAN.

However, C-RAN involves a huge overhead on the fronthaul link because very high bandwidth is required on the common packet radio interface (CPRI) between the RRH and the BBU pool to transmit In-phase and Quadrature (IQ) data. For instance, in order to carry a 2x2 MIMO, 20 MHz LTE signal, 2.5 Gbps of bandwidth is needed on the CPRI. At the same time, strict constraints on latency and jitter have to be fulfilled, in particular, the RTT delay of user data should be less than 5μs [24], and jitter should be less than $65ns$ [1]. Several transport options are possible for CPRI transport such as Dedicated fiber, Optical transmission network (OTN), Passive optical network (PON) and Microwave Radio (MWR). For PSN scenarios, as fiber is likely not to be available, microwave transport is usually the best option for CPRI, provided that the distance between RRH and BBU is less than 1 kilometer. Note that MWR can only support a subset of the CPRI line bit rate options. But with 3:1 compression of CPRI, it is possible to fronthaul a 2x2 MIMO LTE 3-sector RRH site under full load over two times 1 Gbps MWR links [17].

3.3 Resilient Backhaul solutions

In case of major emergency situations, Evolved Universal Terrestrial Radio Access Network (E-UTRAN) may become isolated from the core network and the backhaul access (i.e., the X2 air interface in LTE) has to be rebuilt on the fly. The 3GPP 22.897 specification [2] describes different public safety scenarios and the corresponding requirements to maintain basic services to users. Note that the problem of isolated eNBs is also frequent in moving cells scenarios, where the connectivity remains limited to only a subset of eNBs that can still communicate to each other through the remaining part of the backhaul. Recently a few solutions have been proposed to re-establish the communication among different network partitions.

In [3], the concept of evolved User Equipments (eUEs) is proposed where eUEs are used as relays between eNBs and are able to be associated with and convey trafic from multiple eNBs, making possible backhaul access to moving cells or core-isolated cells as illustrated in Figure 5. In other words, eUEs play the role of a virtual MIMO antenna with collaborative transmission, which could be implemented as a new coordinated multipoint (CoMP) mechanism. In this way, a virtual overlay wireless mesh can be formed on top of the LTE cellular topology.

Another solution is proposed in [9] for the scenario where eNBs are in range of each other. This proposal introduces the concept of enhanced evolved Node B (e2NB) that leverages the existing LTE air interface to allow communication between eNBs through a Tx/Rx transmitter, and this, without requiring modifications of the LTE components and protocols.

As shown in Figure 6, the architecture of e2NB adds to the eNB different LTE components that makes it still operational in the case it is isolated from the core network. Examples of components include the Mobile Management Entity (MME) and the Home Subscriber Server (HSS) components, but also two new functions: (1) Virtual UEs (vUEs) that are deployed as a service by the e2NB to

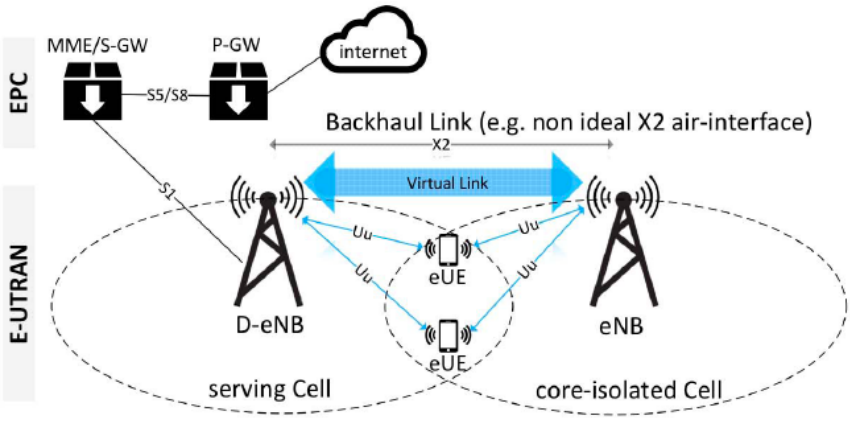

Figure 5: eUE. Source:[3]

establish a connection with some of neighboring e2NBs; and (2) a Coordination and Orchestration Entity (COE) that handles the inter-e2NB communication and coordinates with other COEs to establish the network topology and optimize the network. Furthermore, the COE manages the IP addressing space and performs mesh routing algorithms.

Note that the COE functionality could be implemented in a software defined networking (SDN)-based network control plane as well as the CoMP functionality [5].

[13] proposes a similar software architecture design to enhance the resilience of LTE networks and enable the operation of isolated base stations (eNB) to serve in PSNs. The authors introduce the notion of Hybrid-eNB (HYeNB) that includes the usual entities of an eNB, collocated with a flexible management entity (FME) handling the main Evolved Packet Core (EPC) functions required to serve the attaching user equipments (UEs). The HYeNB uses its backhaul link only to synchronize the UE context with the physical EPC. The virtual EPC inside the FME is pictured in Figure 7. It is made of a gateway-agent (GW-A) that manages the user plane functionalities, a Mobility Management Entity-Agent (MME-A) that manages the control plane functionalities, including virtual X2 interfaces and handover procedures, and a D2D-Agent (D2D-A) that manages the mechanisms to enable D2D communications, as explained below. A link management unit (LMU) manages the link with the physical EPC through a single or multi-hop connection. A routing management unit (RMU) routes the packets in the network and maintains the active path with the physical EPC. A topology management unit (TMU) optimizes the topology of a network when it contains several HYeNBs. Moreover, when UEs are not in the coverage of an HYeNB, the authors propose a device-to-device (D2D)

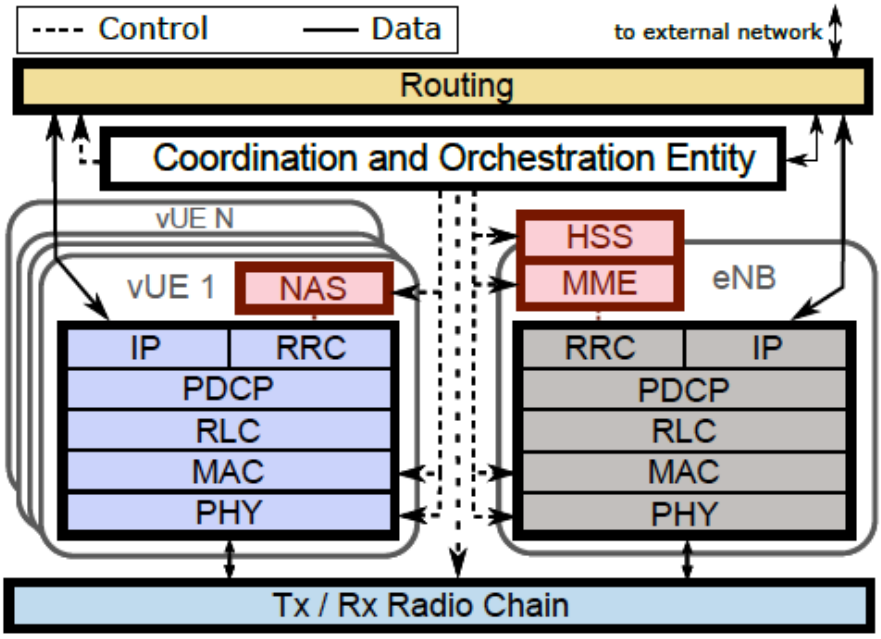

Figure 6: e2NB. Source:[9]

communication mechanism where the head of a group of PS users broadcasts a D-Beacon to create and advertise a D2D network with its neighbouring devices. As soon as one of the UEs recovers the connectivity to an HYeNB, all resources allocated to the D2D communications are disabled.

3.4 SDN-based frameworks for PSNs

3.4.1 Network Embedded On-line Disaster (NEOD)

Network Embedded On-line Disaster (NEOD) is a globally deployable SDN-based network disaster management system that focuses on agility, accuracy, reliability, and scalability issues. It provides abstraction layers to deploy vendor-agnostic event detectors and to facilitate dynamic configuration of network policies. As illustrated in Figure 8, NEOD uses a two-tier architecture: (1) a disaster event detection and filtering segment embedded in an OpenFlow Switch as an OpenFlow firmware extension; and (2) a disaster correlation and detector management segment residing in one or more controllers. The first segment includes Event Detectors, a Dynamic Event Detector Manager, an Event Publisher, and the System Event Adaptation Layer. Event Detectors use configured policies to monitor the disaster events, which are sent by the Event Publisher. In the second segment, the NEOD manager performs correlation of disaster events to provide root cause classification and prediction of events that have been considered as

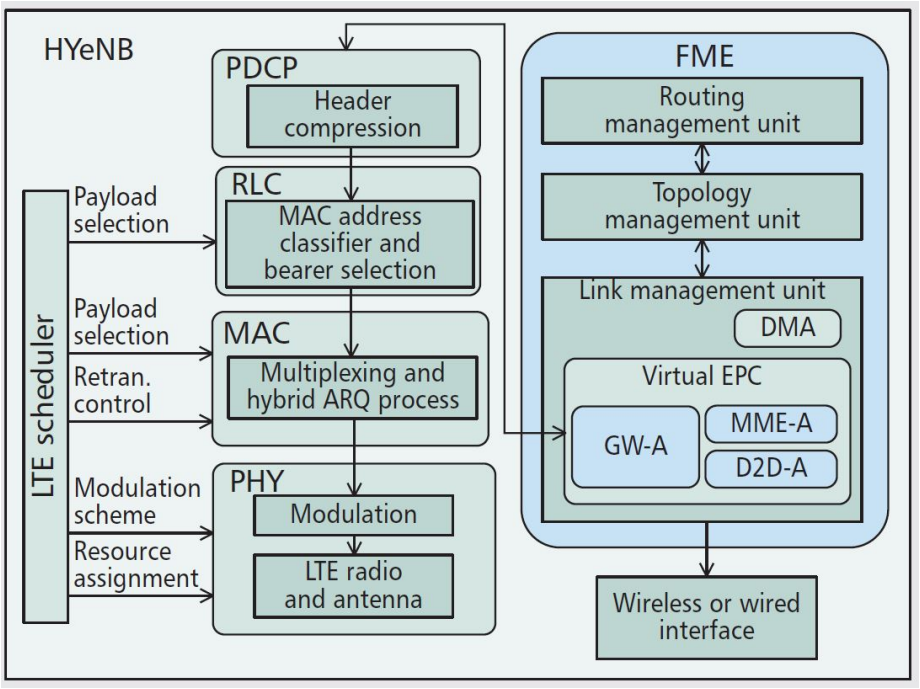

Figure 7: FME software elements and interfaces. Source:[13]

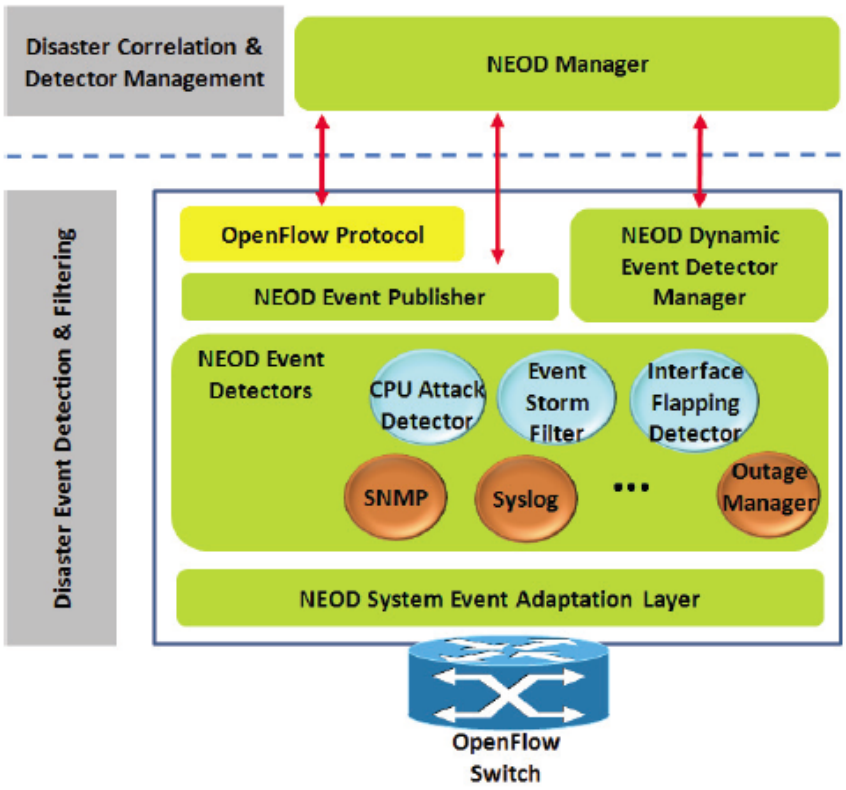

Figure 8: NEOD Architecture. Source:[22]

not scalable or impossible to conduct. Three types of NEOD Disaster event detectors are provided: (1) *new flow attack* consisting in injecting randomly a large number of new flows to an OpenFlow switch; (2) *interface flapping* where a switch interface has a hardware failure that generates alternately "up" and "down" events; and (3) *Event Storm* that can occur in case of multiple status changes on a network object that is containment relationship with a large number of other objects.

3.4.2 Decentralize-SDN (D-SDN)

Decentralize-SDN (D-SDN) [21] is a framework that aims to distribute the SDN control in presence of multiple administrative authorities. It provides both physical and logical control distribution through a hierarchy of controllers composed of main controllers and secondary controllers, as illustrated in Figure 9.

To operate, a secondary controller needs first to be activated by a main con-

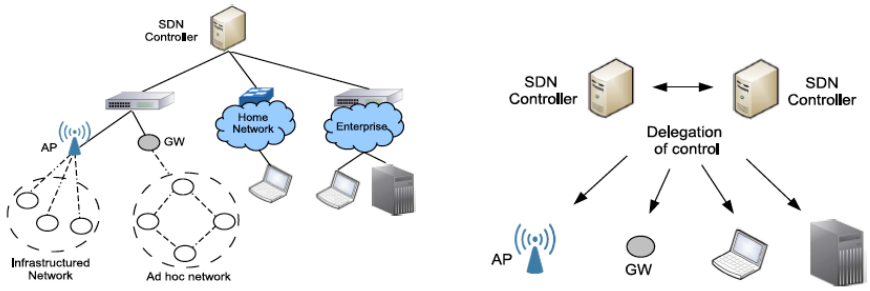

Figure 9: SDN control delegation

troller, which includes secure authorization and control delegation mechanisms. Furthermore, the hierarchical structure of controllers helps in improving control plane availability and fault tolerance.

D-SDN has been applied to a public safety network scenario such as shown in Figure 10 to demonstrate how control decentralization can help in deploying rapidly and in a reliable way emergency communication services.

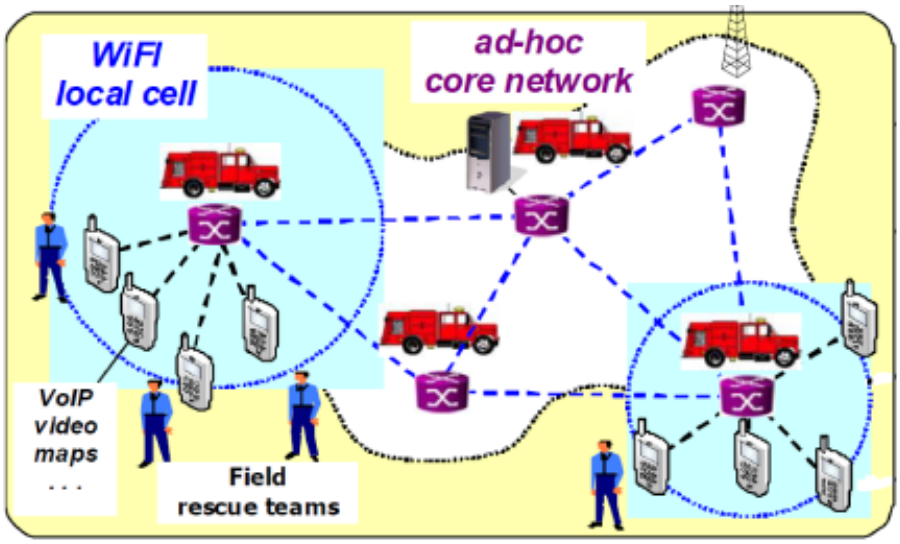

Figure 10: Broadband scenario for inter-agency communication. Source:[7]

The scenario exhibits different public safety authorities that organize themselves for exchanging valuable information regarding an emergency situation. Secondary controllers are running on agency vehicles and serve as gateways to a network of the different agency actors including firefighters and police officers. An agency typically has many decentralized secondary controllers that exchange messages with other agencies' secondary controllers. The D-SDN framework is

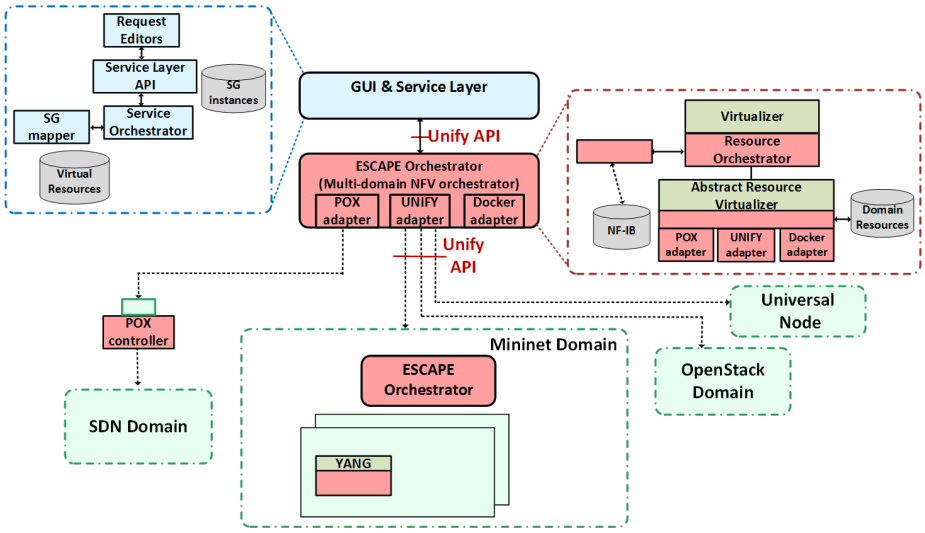

Figure 11: Joint SFC control architecture. Adapted from:[23]

used to provide fault tolerance communication mechanisms. In particular, in such extreme environments, connectivity disruptions are frequent and should trigger a new controller to take over and manage remaining reachable SDN-enabled devices. An algorithm is proposed to elect in a secure way another secondary controller in case the previous one is no more reachable. Such a control delegation is challenging to perform as the system should maintain flow consistency and share flow state between controllers in presence of extreme conditions. Finally, D-SDN provides security mechanisms services which are particularly important in this context, including secure communication with authentication between controllers and secure association between switches and controllers.

3.4.3 UNIFY Service Function Chaining (SFC)

As opposed to ISP or data-center networks that are deployed, operated, and maintained by network engineers, in some situations PSNs will be deployed and operated by emergency services personal that are not engineers. It is therefore essential to simplify the usability of the system and the UNIFY framework offers a first step towards this simplification. The UNIFY common orchestration framework [23] proposes a joint cloud and resource virtualization Application Programming Interface (API) to optimize resource management in multi-technology domains, including legacy technologies. The proof-of-concept (PoC) pictured in figure 11 supports a recursive orchestration mechanism and automated dynamic service creation. A network function (NF) in a client virtualization can also be replaced with the inter-connection of several NF subcomponents, chained to perform the initial function objective. The core of the

framework is the ESCAPE global Orchestrator, designed to meet the requirements of the joint SFC control plane. It supports recursive orchestration, the UNIFY resource abstraction model and can address different technological domains via Controller Adapters. A GUI and Service Layer sits on top of the northbound interface to the Orchestrator. It revolves around a Service Orchestrator, which uses a Service Graph mapper to map the service requests (bandwidth, delay) defined by the consumers of the UNIFY resource service into a Virtualizer. The global Orchestrator manages the virtualized resources and network functions. It passes the service requests to an Abstract Resource Virtualizer over different NF execution environments through specific domain adapters via its southbound interface. The lower layer of the PoC demonstrating the SFC is mainly implemented in the Mininet domain, even though OpenFlow or a standard Universal Node can also be accommodated. In Mininet, the YANG component contains the data model of the Virtualizer. A dedicated local orchestrator identical to the global Orchestrator manages the NFs and deploys the service chains over the domain resources. It takes advantage of recursive algorithms over the Virtualizer-Manager interface to benefit from the NF decomposition.

4 Conclusion

This report presented the evolution of PSNs from voice communications as defined in TETRA or P25 networks towards the more recent networking technologies. Starting from the detailed example of an earthquake emergency scenario, the main requirements of future PSNs could be derived. Fast network deployment, flexibility in the control of the communication flows for robustness, reliability, secure resources management, or resilience are the main features that naturally bring forward the recent softwarization and virtualization of the networks, as defined in SDN, NFV or SFC novel technologies. A set of applications or PSN frameworks that take advantage of these new technologies, either at node or at system level has been presented, involving the RAN, the backhaul, and the service layer. They picture how software networks help complying with the critical requirements of PSNs, benefiting from the clear separation between data and control plane, the faster convergence of newly installed networks, the centralization of policy decisions, and the flexibility of reconfiguring network functions in case of overload or hardware damage. PSNs are currently moving towards existing technologies to provide their users with capabilities equivalent to commercial data networks. Softwarization and virtualization will be their next step.

References

[1] 3GPP. Base Station BS Radio Transmission and Reception (Release 10). TS 36.104, 3rd Generation Partnership Project (3GPP), 2010.

[2] 3GPP. Study on isolated Evolved Universal Terrestrial Radio Access Network (E-UTRAN) operation for public safety. TR 22.897, 3rd Generation Partnership Project (3GPP), 2014.

[3] A. Apostolaras, N. Nikaein, R. Knopp, A. M. Cipriano, T. Korakis, I. Koutsopoulos, and L. Tassiulas. Evolved user equipment for collaborative wireless backhauling in next generation cellular networks. In *SECON 2015, 12th IEEE International Conference on Sensing, Communication and Networking, June 22-25, 2015, Seattle, USA*, 06 2015.

[4] A. Checko, H. L. Christiansen, Y. Yan, L. Scolari, G. Kardaras, M. S. Berger, and L. Dittmann. Cloud ran for mobile networks - a technology overview. *Communications Surveys & Tutorials, IEEE*, 17(1):405–426, 2014.

[5] N. Cvijetic, A. Tanaka, K. Kanonakis, and T. Wang. Sdn-controlled topology-reconfigurable optical mobile fronthaul architecture for bidirectional comp and low latency inter-cell d2d in the 5g mobile era. *Optics express*, 22(17):20809–20815, 2014.

[6] T. Doumi, M. Dolan, S. Tatesh, A. Casati, G. Tsirtsis, K. Anchan, and D. Flore. LTE for public safety networks. *Communications Magazine, IEEE*, 51(2):106–112, 2013.

[7] EADS Defence Security Systems. CHORIST. Technical Report SP0.R7, FP6, Sixth European Framework Programme, 2009.

[8] ETSI. Reference scenario for the deployment of emergency communications; Part 1: Earthquake. TS 103 260-1, European Telecommunications Standards Institute (ETSI), 2015.

[9] R. Favraud and N. Nikaein. Wireless mesh backhauling for LTE/LTE-A networks. In *MILCOM 2015, 2015 IEEE Military Communications Conference, October 26-28, 2015, Tampa, FL, USA*, Tampa, ÉTATS-UNIS, 10 2015.

[10] First Responder Network Authority. Why Firstnet, http://www.firstnet.gov/about/why, 2012.

[11] S. Forge, R. Horvitz, and C. Blackman. Is commercial cellular suitable for mission critical broadband? *A study prepared for the European Commission DG Communications Networks, Content & Technology by SCF Associated Ltd*, 2013.

[12] O. N. Foundation. Optical transport working group otwg. In *Open Networking Foundation ONF*, 2013.

[13] K. Gomez, L. Goratti, T. Rasheed, and L. Reynaud. Enabling disaster-resilient 4g mobile communication networks. *Communications Magazine, IEEE*, 52(12):66–73, December 2014.

[14] S. Jain, A. Kumar, S. Mandal, J. Ong, L. Poutievski, A. Singh, S. Venkata, J. Wanderer, J. Zhou, M. Zhu, et al. B4: Experience with a globally-deployed software defined WAN. In *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, pages 3–14. ACM, 2013.

[15] M. Kobayashi, S. Seetharaman, G. Parulkar, G. Appenzeller, J. Little, J. van Reijendam, P. Weissmann, and N. McKeown. Maturing of OpenFlow and Software-defined Networking through deployments. *Computer Networks*, 61:151–175, Mar. 2014.

[16] D. Kreutz, F. Ramos, P. Esteves Verissimo, C. Esteve Rothenberg, S. Azodolmolky, and S. Uhlig. Software-defined networking: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 103(1):14–76, Jan 2015.

[17] J. Lorca and L. Cucala. Lossless compression technique for the fronthaul of lte/lte-advanced cloud-ran architectures. In *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2013 IEEE 14th International Symposium and Workshops on a*, pages 1–9. IEEE, 2013.

[18] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner. Openflow: enabling innovation in campus networks. *ACM SIGCOMM Computer Communication Review*, 38(2):69–74, 2008.

[19] NOKIA. LTE networks for public safety services. *White paper*, 2014.

[20] B. Nunes, M. Mendonca, X.-N. Nguyen, K. Obraczka, and T. Turletti. A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks. *Communications Surveys Tutorials, IEEE*, 16(3):1617–1634, Third 2014.

[21] M. Santos, B. Nunes, K. Obraczka, T. Turletti, B. T. de Oliveira, C. B. Margi, et al. Decentralizing sdn's control plane. In *39th IEEE Conference on Local Computer Networks (LCN)*, pages 402–405, September 2014.

[22] S. Song, S. Hong, X. Guan, B.-Y. Choi, and C. Choi. Neod: network embedded on-line disaster management framework for software defined networking. In *Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on*, pages 492–498. IEEE, 2013.

[23] B. Sonkoly, J. Czentye, R. Szabo, D. Jocha, J. Elek, S. Sahhaf, W. Tavernier, and F. Risso. Multi-domain service orchestration over networks and clouds: a unified approach. In *Proc. ACM SIGCOMM, London, United Kingdom*, pages 377–378. ACM, 2015.

[24] X. Wang. C-ran: the road towards green ran. *China Communications Journal*, 2010.

[25] W. Xia, Y. Wen, C. H. Foh, D. Niyato, and H. Xie. A survey on software-defined networking. *Communications Surveys Tutorials, IEEE*, 17(1):27–51, Firstquarter 2015.