STSM Title: 5G Networks in disaster based situations

STSM Applicant: Eryk Schiller

Working Group: WG3

STSM Host: EURECOM, Campus SophiaTech, 450 Route des Chappes, CS 50193, 06904 Biot, Sophia Antipolis CEDEX France

Purpose of the visit

US federal and EU authorities have identified 4th Generation Long Term Evolution (LTE) as a basis for public-safety (PS) networks that will provide the first seamless communication channels between agencies across geographical locations in tactical and emergency scenarios [Lie15]. From Release 11, the Third-Generation- Partnership-Project (3GPP) has focused its efforts on the specification and development of dedicated public safety broadband networks. The main interest is put on scalability, robustness, and resiliency to failures in networks supporting communication requirements of emergency services. 3GPP investigates scenarios and requirements for an Evolved Universal Terrestrial Radio Access Network (E-UTRAN) that operates with limited or no access to the Evolved Packet Core (EPC).

During this STSM visit we are supposed to classify the result of various critical situations affecting the 5G network that lead to a failed communication service. We argue that the network could still function using the Information Centric Networking (ICN)/Delay Tolerant Networking (DTN) paradigms in the case of an operational eNB working in the failed S1 or EPC scenario. During this STSM we target the provisioning of a disconnected E-UTRAN system. As the Network Function Virtualization (NFV)/Software Defined Networking (SDN) [Abd16, Cho14] are currently envisioned as an essential building block of 5G networks of the future, we will explore the use of NFV/SDN to deploy self-configurable PS networks working in the disconnected core scenario.

Description of work carried out during the STSM

A typical E-UTRAN network can fail in various critical situations that can cause damages to various components of the 5G ecosystem. It results in a destroyed eNB, failed S1 interface disrupting the control and data plane, or damaged EPC. Note that when a fully functional eNB looses its connection to the core, it stops providing RAN. This situation can be a result of a failed S1 or EPC scenario (c.f., Fig. 1, 2). Strong protection mechanisms (such as independent power supplies, uninterruptible power supplies, etc.) can be used for protecting legacy mobile telephony systems such as en eNB.

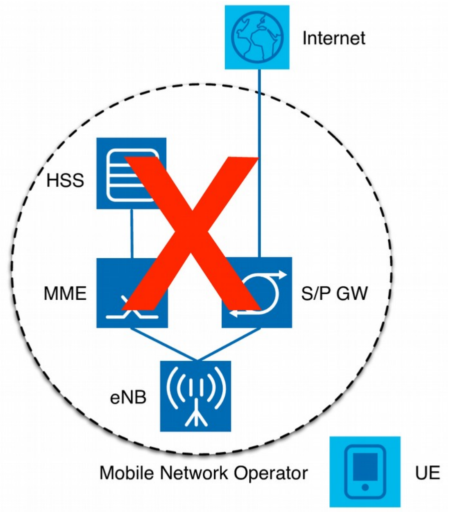

Figure 1: Failed EPC case

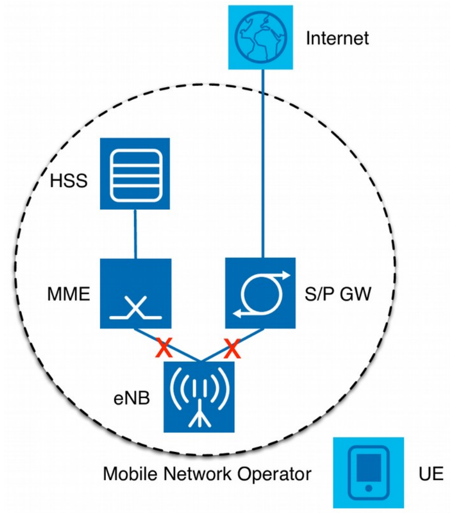

Figure 2: Faild S1 case

Let us now focus on Mobile Edge Computing (MEC). The architecture of a MEC system, which is described in the ETSI white-paper [ETS14], is illustrated in Figure 3. The primary purpose of the MEC server is to run MEC applications that improve user quality of experience such as caching, online gaming, augmented reality, etc. Due to MEC, the base station can already actively cooperate in the DTN/ICN information dissemination by instantiating DTN/ICN based services as Virtual Network Functions (VNFs) [Sou16].

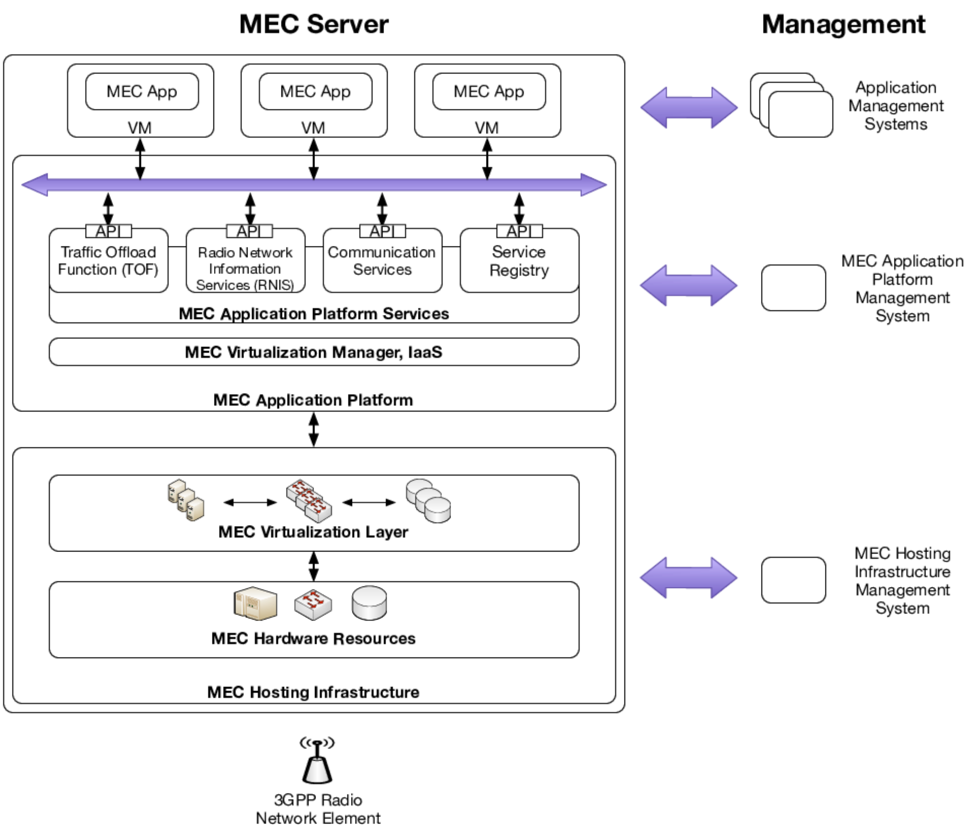

Figure 3: ETSI MEC architecture

Due to strong protection mechanisms, a MEC capable macro eNB site can independently operate (of the core) for a long time after the critical event occurs, when the network core failed or the S1 interface malfunctioned. A macro MEC-enabled eNB is the main architectural element of the system. In the ordinary situation, when the network core is reachable, our MEC eNB site runs a software based Base-Band-Unit (BBU), which is a software part of an eNB that provides E-UTRAN and communicates with the operator network core to provide mobile access.

Whenever a local Application Management Unit discovers that an macro eNB station becomes disconnected from the core network, and that the eNB is not able to operate as an isolated eNB, it starts the recovery procedure to provision a new communication service. Such a service is deployed as a bundle of VNFs that defines the required network services, namely eNB, local S+P GW, MME, and HSS, and PS, and leverages the MEC platform when available to provide a fast network recovery and at the same time offer additional services (c.f., Figs.4, 5). User information is maintained either by replicating the HSS database if possible, or by provisioning the known IMSI (range) without necessarily the operators key and sequence numbers. Note that the authentication procedure can also be relaxed so as to accept all the attach procedures. All the VNF functions are instantiated on the the same edge cloud. The BBU has to be re-instantiated to acknowledge local copies of the MME, SPGW, HSS providing core network services. The MME, SPGW, and HSS are minimal services of a small footprint. They provide basic LTE functions and connect UEs attached with the macro eNB. Due to the basic core function, the UEs attached to the same eNB can communicate directly with the help of the PS VNF. The PS VNF is based upon DTN and/or ICN applications such as CCNx1 , or DTN22 . It is a communication end-point and a relay between other clients instantiated on Ues.

Results

In Fig. 6, we gather instantiation times for the PS service bundle (MySql is a supporting system for HSS). We tested two scenarios, when dtn (i.e., PS instance), mysql, epc, hss were instantiated on KVM and LXC respectively. In both scenarios, however, the eNB runs on the host as a bare metal service. This is to simplify the setup as in the bare metal mode, a pass-through between RF equipment and the container/VM is not necessary and the BBU can enjoy real-time capabilities of the host kernel. We use a single host machine with Intel 3.20 GHz quad core CPU and 16 GB RAM. The services use 1 thread, 1 GB RAM; 1 thread 1 GB RAM; 4 threads 8 GB RAM; 1 thread, 2 GB RAM; 1 thread, 1 GB RAM for mysql, hss, enb, epc, and dtn resp.

We have developed an PS architecture for a macro eNB with MEC operating in a disconnected core scenario. MEC successfully establishes the whole LTE stack and provisions necessary PS services such as a DTN agent at the edge. The instantiation time is of about 650 s for KVM and 400 s on a typical commodity hardware, what is reasonable. Our solution can significantly improve the PS communication at the network edge. Future works include packaging the modules, thus improving instantiation time. We will also target other radio technologies such as WiFi.

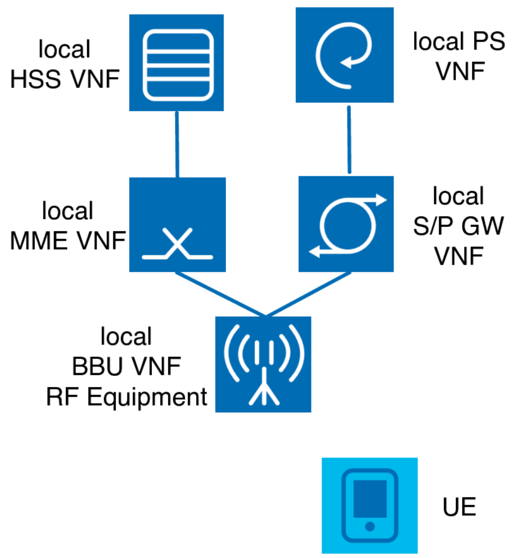

Figure 4: PS service bundle.

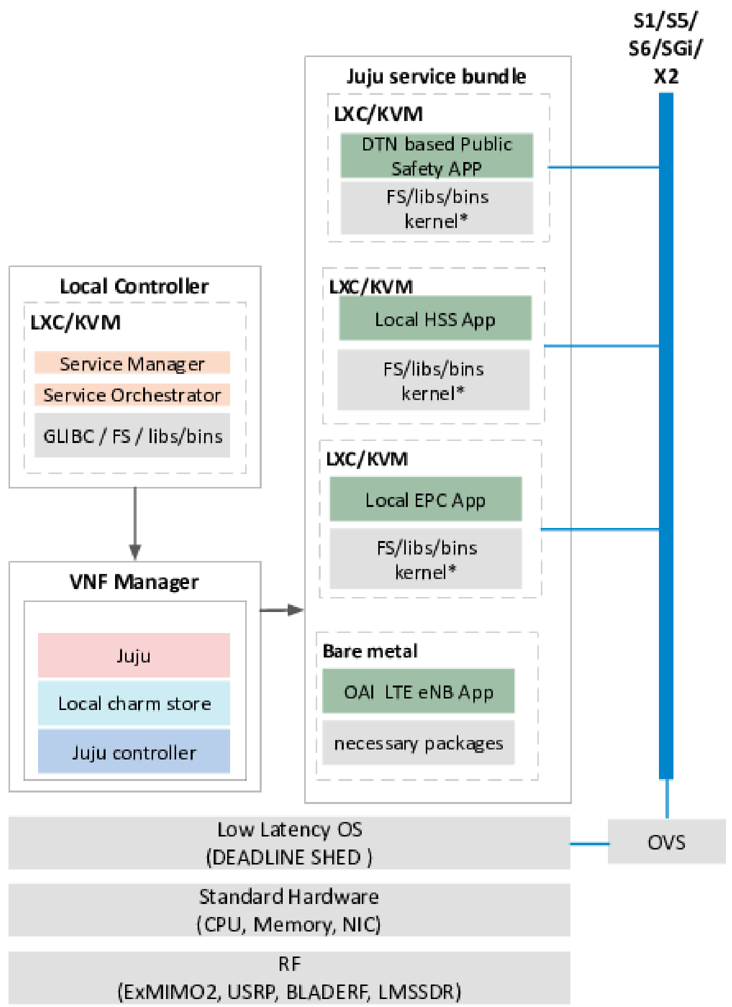

Figure 5: Software architecture.

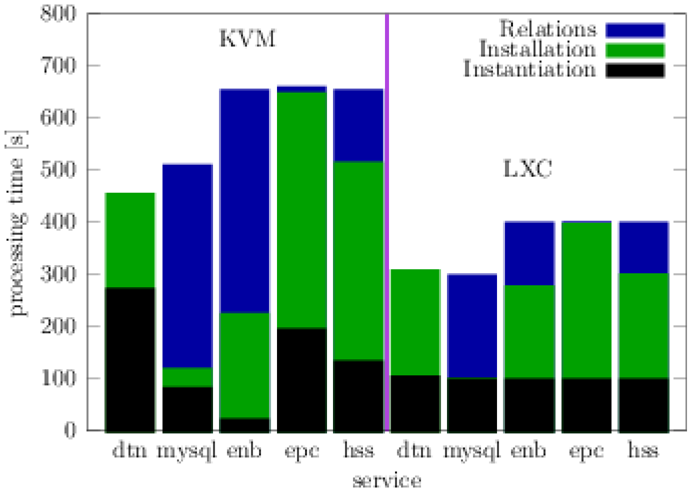

Figure 6: Instantiation time of the PS VNF bundle.

Publications

Submitted: Eryk Schiller, Eirini Kalogeiton, Torsten Braun, Andre Gomes, Navid Nikaein, "**Orchestration of DTN/ICN based services on Edge Clouds for Public Safety in 5G Networks**", **IEEE ICC 2017 NGNI**.

Envisioned a book chapter with an extended version of the ICC paper submitted for publication in a book D. Câmara and N. Nikaein, "**Wireless Public Safety Networks**", vol 1-3, **Elsevier B.V**., 2015-2017.

Future Projects

INRIA, EURECOM, and the University of Bern registered a project entitled "**SLA driven Cross-plane management for wireless networks towards 5G Network Slices"** using the PCRI funding instrument (Projets de recherche collaborative – Internationale) with FR-ANR (Agence Nationale de la Recherche) and CH-SNF (Swiss National Science Foundation).

References

[Abd16] S. Abdelwahab, B. Hamdaoui, M. Guizani, and T. Znati, "Network function virtualization in 5G," In: IEEE Communications Magazine , vol. 54, no. 4, pp. 84–91, 2016.

[Cho14] H. H. Cho, C. F. Lai, T. K. Shih and H. C. Chao, Integration of SDR and SDN for 5G, In IEEE Access, vol. 2, no. , pp. 1196-1204, 2014.

[ETS14] M. Patel, B. Naughton, C. Chan, N. Sprecher, S. Abeta, and A. Neal, Mobile-edge computing – introductory technical white paper, ETSI Sep. 2014.

[Lie15] R. Liebhart, D. Chandramouli, C. Wong, and J. Merkel, LTE for Public Safety. John Wiley & Sons, Ltd, 2015

[Sou16] B. Sousa, L. Cordeiro, P. Simoes, A. Edmonds, S. Ruiz, G. A. Carella, M. Corici, N. Nikaein, A. S. Gomes, E. Schiller, T. Braun, and T. M. Bohnert, "Toward a fully cloudified mobile network infrastructure,", IEEE Transactions on Network and Service Management, vol. 13, no. 3, pp. 547-563, Sept 2016.