

Research Article

Multihoming for Mobile Internet of Multimedia Things

Titus Balan, Dan Robu, and Florin Sandu

Department of Electronics and Computers, “Transilvania” University of Brasov, Brasov, Romania

Correspondence should be addressed to Titus Balan; titus.balan@unitbv.ro

Received 28 April 2017; Revised 14 July 2017; Accepted 6 August 2017; Published 26 September 2017

Academic Editor: Bartolomeo Montrucchio

Copyright © 2017 Titus Balan et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Mobility, redundancy, and bandwidth requirements are transforming the communication models used for IoT, mainly in case of Critical Communications and multimedia streaming (“IoMT, Internet of Multimedia Things”), as wireless video traffic is expected to be 60–75% of the global mobile traffic by 2020. One of the characteristics of 5G networks will be the proliferation of different/heterogeneous radio networks (virtualized radio access networks, RAN, new energy-efficient radios, femtocells, and offloading capabilities) and the possibility for IoT objects to connect and load-balance between dual and multiple RANs. This paper focuses on the possibility of using LISP (Locator Identifier Separation Protocol) for multihoming and load-balancing purposes and presents an illustrative scenario for the case of mobile IoT (e.g., the “things” part of vehicular or public transportation systems, PTS) that are also intensive bandwidth consumers, like the case of connected multimedia “things.” We have implemented and tested a demonstrator of a mobile LISP IoT gateway that is also integrated with Cloud-based video analytics.

1. Introduction

IoT devices are supposed to be small sized objects equipped with a limited amount of power resources. That is why 3GPP also defined Narrow-Band IoT (NB-IoT) [1] for low bandwidth and low power consuming devices. However, there are some IoT applications [2] that manifest an increased request for redundancy and some also for a greater throughput. And here we can mention the needs of Internet of Multimedia Things (IoMT) [3] applications and also the IP broadband requirements from Mission Critical Communications applications [4] that are enhanced with IoT communication.

Smart IoT multihoming and multiple-RAN connectivity management, including automatic air interface selection and optimal weighted load-balancing between interfaces, are challenges for the reliability of future networks. Without reliable mechanisms for multihoming and load-balancing of multiple interfaces, all the Mission Critical Communication could not function.

Mobility, redundancy, and bandwidth requirements may be transferred, in an IoT ecosystem, from the sensors and devices to the IoT gateway element, but wherever it resides, the redundancy and load-balancing function of mobile IoT is dependent on the mechanisms for RAN multihoming.

Although 3GPP has some own initiatives in the area of mobility, LIPA (Local IP Access), SIPTO (Selected IP Traffic Offload), IFOM (IP Flow Mobility), MAPCON (Multiple Access PDN Connectivity), or SI-flex (meshed SI interfacing), each solution having some drawbacks, this paper focuses on the opportunities of using LISP [5]. Recognized as a serious candidate for 5G standardization and intensively backed-up by a IETF (Internet Engineering Task Force) Work Group, LISP offers mobility, multihoming, and load-balancing that have the advantage to be applied with no changes in the Internet architecture (directly at the mobile IoT element) [6] and furthermore can be perfectly matched with SDN (Software Defined Networks) that represent another highlight of 5G architectures.

IoT mobility gets a new dimension when we discuss the implementations of Mobile Edge Computing (MEC) [7] and Fog Computing for IoT, as the processing can take place distributed, where the objects are, thus reducing communication delays to a central processing Cloud.

In this case, IoT mobility could refer to

- (i) the mobility of “things” (IoT gateways, devices, and sensors) following the global understanding of host/user mobility;

- (ii) the mobility of the virtual machines (VMM, Virtual Machine Mobility) from one Edge Cloud to the other, concept also known as “Follow-Me Cloud,” a method for interworking of federated clouds and distributed mobile networks [8].

The LISP protocol is a recognized solution for both the above-mentioned mobility cases, thus being differentiated from other mobility solutions. Furthermore, it is a very good option for multihoming, among other multihoming solutions that will be mentioned in a latter section.

Although LISP is a recognized mobility solution, there are no implementations focused on using LISP for IoT systems. This paper is focused on identifying the advantages of LISP for IoT and describes an implementation for IoT of the LISP architecture based on the open-source LISP implementation Open Overlay Router (OOR) [9] and IBM Watson [10] as IoT platform. The implemented use-case is focused on IoMT, an IoT network based on multimedia sensors with video analytics support in the Cloud. Furthermore, our use-case takes into consideration multiple operator solutions for multimedia streaming based on LISP.

This paper is organized as follows: the first part is the introduction; the second section makes a fast description of the related work in respect to multihoming and LISP usage for this use-case, while the third and fourth sections describe briefly the LISP protocol and the advantages of using LISP for IoT and the methods to handle IoT mobility and multihoming with LISP. The next part details our experimental implementation of an IoT gateway having as base the Open Overlay Router LISP implementation, while the sixth section handles the IBM Watson for data analytics. Last two parts describe the methodology used and the experimental results for video streaming in a mobile, multihomed, and load-balanced environment. Conclusions and plans for future works are presented in the last section.

2. Related Work

There are already different methodologies to address the important issues of multihoming; part of the related multihoming methodologies make use of the LISP protocol that is also in the focus of our approach [11–13]. In this section, as we review the existing approaches, we gradually try to point out the novelty of our solutions and the advancement with respect to the state of the art.

Important state-of-the-art reference papers [14–16] differentiate between the end-host and end-site multihoming. End-site multihoming has gained more attention than end-host multihoming, mainly due to the routing scalability problems that Internet is facing and because of the ascension of Mobile Edge Computing. Edge computing will be an important part of our implementation, as described in the following.

LISP is mentioned in [15] as a method for end-site multihoming but an evaluation of its efficiency is not included; our paper aims to bring such an evaluation. Reference [15] also considers multihoming based on transport protocols, including the well-known method of Stream Control Transmission Protocol (SCTP) multihoming, evaluated in [16, 17]. SCTP,

despite having some advantages, has the main disadvantage that it operates at the transport layer. This means that the applications must be written from the beginning to support SCTP or the existing applications must be rewritten. This is where LISP does a better job: the applications remain the same; also a big part of the network is unchanged. SCTP had a big traction in telecommunications but outside of this field was not promoted at all.

Although not included in this category by the survey in [15], NEMO (Network Mobility) is also considered in the related work for end-site mobility [18], as it manages the mobility of a network of nodes that are typically moving in tandem [19]. Separation between location and identity for the case of multihoming is also mentioned in [20], but using the ILNPv6 protocol.

LISP-MN (for Mobile Networking) [21] is a lighter version of LISP. Compared to Mobile IP v4 or v6, there are no required Home Agents/Foreign Agents but LISP-MN has also less routing capabilities (as routing is needed for a single destination).

Different scenarios for multihoming and mobility testing based on LISP are proposed in [5] and RFC 6830 bis, as well as in [22]. Testing LISP for multihoming purpose was also performed in [23]: a performance evaluation of LISP multihoming was accomplished in a controlled environment. The LISP implementation used in [23] is the Open Overlay Router (OOR) [9], the same implementation to be used also in this paper. While [23] aims to demonstrate the accuracy of the OOR implementation, with respect to the configurability of load-balancing weights and, nevertheless, to the behavior of LISP for data transfers in a static (nonmobile) environment, our paper will focus on a mobile IoT environment. As shown in [24], OOR supports both LISP and LISP-MN by implementing both the mobile node, MN, and a lighter version of xTRouting.

LISP was also proposed as a mobile solution for multihoming in Mission Critical Communications [25] for the representative ATN (Aeronautical Telecommunication Network) use-case [26, 27].

A LISP assessment was done in Deutsche Telekom Labs in the BOWL Testbed [28], using a LISP implementation developed at “Technische Universität Berlin.” Testing was done in both static and mobile environments (where clients roam from one node to another). However, most of the results are compared in the BOWL IP-in-IP configuration (which consists in adding an extra IP header to the IP packets, which contains the tunneling information) and not with other multihoming “classical” solutions (e.g., SCTP). The mobility testing is based only on Wi-Fi testing. In respect to this related work, our approach aims for real equipment testing (RET) of LISP, “in the field” of a real mobile environment (using two or more mobile operator networks) that are suitable for the heterogeneous IoT elements. As shown in the following, RET will take benefit of high-performance professional instrumentation; the radio coverage maps (for each of the multihomed networks) that we used were not considered up-to-date as a baseline for testing of multihomed LISP solutions. Multihoming was separately evaluated for mobile vehicular networks, but not based on LISP [29]. We

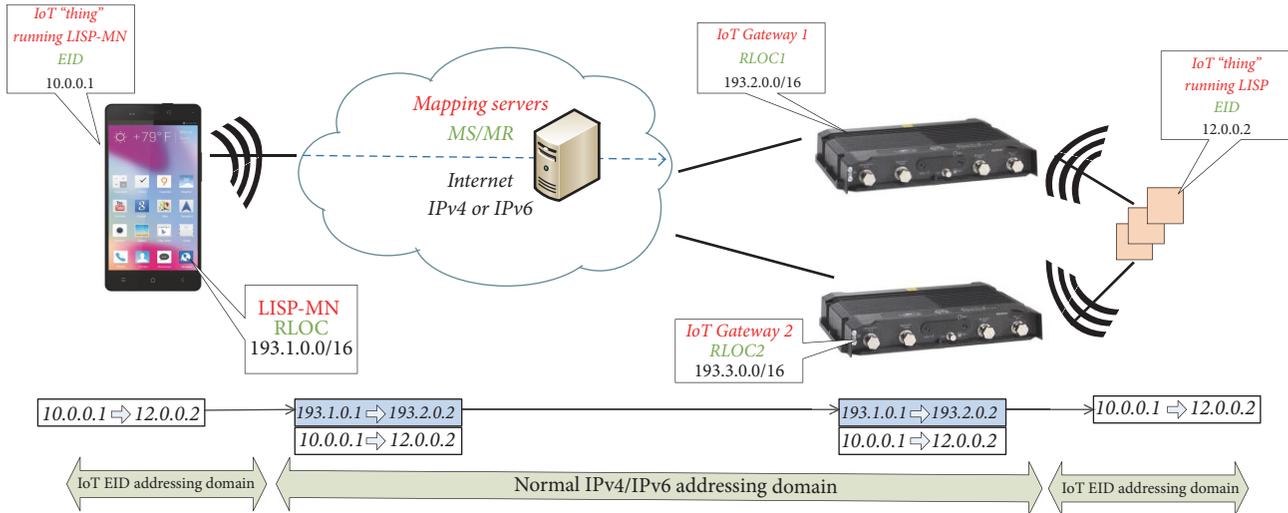


FIGURE 1: LISP implementation example: LISP-MN runs on the mobile device on the left side, while LISP multihoming scenario with multiple IoT gateways is visible on the right side.

can see that the parameters of the signal (strength, SNR, etc.) in urban areas vary a lot [30]. Therefore, an analysis is needed before any bandwidth tests are performed for assessing the mobile test environment (included in our research based on professional tooling).

Another LISP evaluation [31] was performed for Android implementations of Open Overlay Router [9] (former LISP-mob). The important conclusion of this paper is that, compared with standard IPv4 traffic, LISP has almost the half of the relative standard deviation versus IP: this means that communications over LISP tunneling are very stable and this has obvious good consequences in terms of channel throughput, despite the delay introduced by tunneling/encapsulation.

The specialized literature lacks testing of LISP multihoming in mobility scenarios; the previously published LISP multihoming tests were performed only in the above-mentioned controlled lab environments (even the Android case [31] does not mention mobility testing) or not with complex applications, like video streaming (most of the previous tests were oriented on ping, ftp, or BitTorrent transfers).

So, at the application level, [28] and [23] are using benchmarking methods for assessing the transfer rate by downloading torrent files. In this respect, our approach is focused on applications that need network performance based on aggregated bandwidth of different Internet providers. Thus, our evaluation methods are going towards the multimedia streaming (more specific the WebRTC case) and to the IoMT paradigm. We aim to promote decentralization of LISP controls: our demonstrator has an IoT gateway implemented on a Single Board Computer.

IoT multihoming should be seen also from the perspective of mobility protocols. Though LISP is considered a mobility protocol, the latest surveys on mobility management solutions for IoT [32] do not mention LISP as an option. The only aspect where LISP was assessed for IoT usage is not mobility but security (details will be given in the following, Section 4.4).

Concluding on the advancement with respect to the state of the art, our paper has the goal to evaluate LISP for IoMT in a real mobility environment over multihomed mobile telecommunication networks using bandwidth consuming applications. The paper has an important heuristic (practical) value and presents implementation and methodical steps that aim to be considered as a valuable “best practice.”

3. An Overview of LISP

LISP is a network architecture and a set of network-layer based protocols developed by the IETF “LISP Working Group” in RFC 6830 [5] that documents the separation of IP addresses into two new numbering spaces: Endpoint Identifiers (EID-s) and Routing Locators (RLOCs) [33]. The EID identifies the nodes that are connected to the network. The RLOC identifies the location by using the traditional addressing schemes: IPv4 and IPv6. Most of the time, the RLOC is the public address of the routers or gateways [34]. By introducing this separation, new capabilities for mobility, scalability, and security become available [35].

The LISP architecture, based on the “map-and-encapsulate” paradigm, implements a mapping process that is transparent for the users: the RLOCs are responsible for looking up the mapping between the destination EID-s and the corresponding destination RLOC. The key of the system is based on the distributed mapping system, similar to DNS (Domain Name System): MS (Map Server) and MR (Map Resolver). The MS stores the mapping between the EID and the RLOC of a LISP Node and it distributes this information in the mapping system. The MR is used to interrogate the MS database: it receives queries for EID-s and it responds with the corresponding RLOC. Map Servers have similar behavior to the Home Agents in Mobile IP.

Figure 1 describes a LISP multihoming scenario for IoT, several IoT gateways having also the role of xTR (Ingress/Egress Tunnel Router), thus having an assigned RLOC [33],

and the IoT devices/sensors keep their identity (EID) no matter their attachment or roaming status in the network. One of the most important advantages of LISP is multihoming, as it is “embedded” in the protocol definition, providing redundancy and load-sharing, and thus IoT device (EID) can be simultaneously connected to two or more IoT gateways (RLOCs).

Furthermore, Figure 1 illustrates in the left side the LISP-Mobile Node option, a LISP option where the mobile node plays the EID and RLOC role simultaneously, at a smartphone level (there are open LISP implementations available for Android).

4. Locator/Identifier Separation Protocol Advantages for IoT

Here are some of the main advantages of using LISP for IoT [34].

4.1. Easiness for End-To-End Installation in the Network and on the IoT Device. As expressed in RFC 6830 no changes are required to either host protocol stacks or the “core” of the Internet infrastructure. The Locator/ID Separation Protocol (LISP) can be incrementally deployed, without a “flag day” [5]. So only some elements/routers in the network need “to know” the LISP protocol (the IoT gateway in case of IoT), or only a mobile device, in case the LISP-MN option of the protocol is used. The rest of the network and the routing in the Internet remain unchanged. There are schemes for LISP to non-LISP addressing and LISP proxy implementations, so that LISP deployment is facile.

LISP is commonly used with IPv4 or IPv6, but it can be used with any other type of addressing for the EID or RLOC addresses, as the key of the routing is part of the DNS-like mapping servers (MS). For IoT this could bring a great advantage; thus the end-to-end addressing of non-IP IoT devices, like, for instance, IEEE 802.15.4 devices, could be possible directly in the IP header as long as IANA (Internet Assigned Number Authority) is supported, without the need of addressing the gateway.

Another advantage of LISP is the support for High-Scale VPN support, with or without encryption.

4.2. Mobility. LISP is a host mobility protocol and a Virtual Machine Mobility protocol [21]. In case of IoT it can be used as host mobility; the EID based addressing is a method for simplification and abstraction of network infrastructure and the RAN used as point of attachment in the network.

Separation between location and identifier is considered and acknowledged as the optimal method for user/host mobility. In [6] a detailed survey and analysis of network architectures based on location/identifier separation are presented. LISP mobility was previously compared to Mobile IPv6 mobility [36]. It can be considered that also proxy mobility, PMIP [37], used in LTE networks [38], is a separation of edge mobility in relation to the core network; mobile hosts keep their IP address as long as they are part of the same proxy mobility domain.

As Virtual Machine Mobility protocol, LISP can be used for the migration of the localized processing function, for

example, the migration of the IoT gateway functions from one RAN Cloud to another. Vehicle-to-vehicle communication and self-driving cars imply a lot of processing that can only be performed at the edge of the network, in the Edge Clouds, in order to minimize the delays. Migration of virtual machines during their run using LISP is a method for the processing power to follow the intelligent devices in IoT. For VMM (Virtual Machine Mobility), the processing power and applications can follow the mobility of the “thing.” The benefits of using LISP for linking the Virtual Machine Mobility to the user mobility were already demonstrated by some experimental work [39]. This can be the advantage for LISP compared to other mobility protocols and correlated with the ascension of edge computing.

Mobility management RFCs proposals also refer to LISP as one candidate solution. “Mobility Management for 5G Network Architectures Using Identifier-Locator Addressing” [40] specification describes the Mobility Management Architecture for 5G Networks Using Identifier-Locator Addressing in IPv6 for virtualized mobile telecommunication networks. Identifier-Locator addressing differentiates between location and identity of a network node, and it is considered the key method for 5G mobility [41].

4.3. RAN Multihoming and Load-Balancing. For redundancy purpose, in case of IoT elements supporting critical infrastructure elements, failover mechanisms are essential in a network that is connected to multiple providers, while still being reachable via the same address (most probably an IPv6 address, but EID addressing is very permissive). LISP implementations allow the setting of prioritization methods (weighting) for the parallel connected RANs networks, though providing load-balancing for enhance throughput, not just back-up connectivity.

When it comes to LISP multihoming, performance evaluation of LISP multihoming was performed in a controlled environment [23]. Our implementation that will be further detailed is making experiments in the mobile environment, using two ISP (Internet Service Providers). We took also benefit of the mobility function of LISP, as our endpoint device (EID) was free to roam; furthermore, the IoT gateways RLOC itself was mobile.

There are also optimization methods for LISP multihoming based on path ranking algorithms [24].

4.4. Security Aspects. LISP was considered as a protocol for IoT and step-by-step analyzed from security conformance point of view based on X.805 standard that proposes three security layers (application, services, and infrastructure); three security planes (end-user, control, and management), which are based on the performed activates over the network, and eight security dimensions to address general system vulnerabilities (access control, authentication, nonreputation, data confidentiality, communication security, data integrity, availability, and privacy) [42, 43].

In [44, 45] a security implementation to LISP protocol has been found. However, this security protocol provides security to xTR (i.e., ITR and ETR) routers and not for devices that are connected to the architecture.

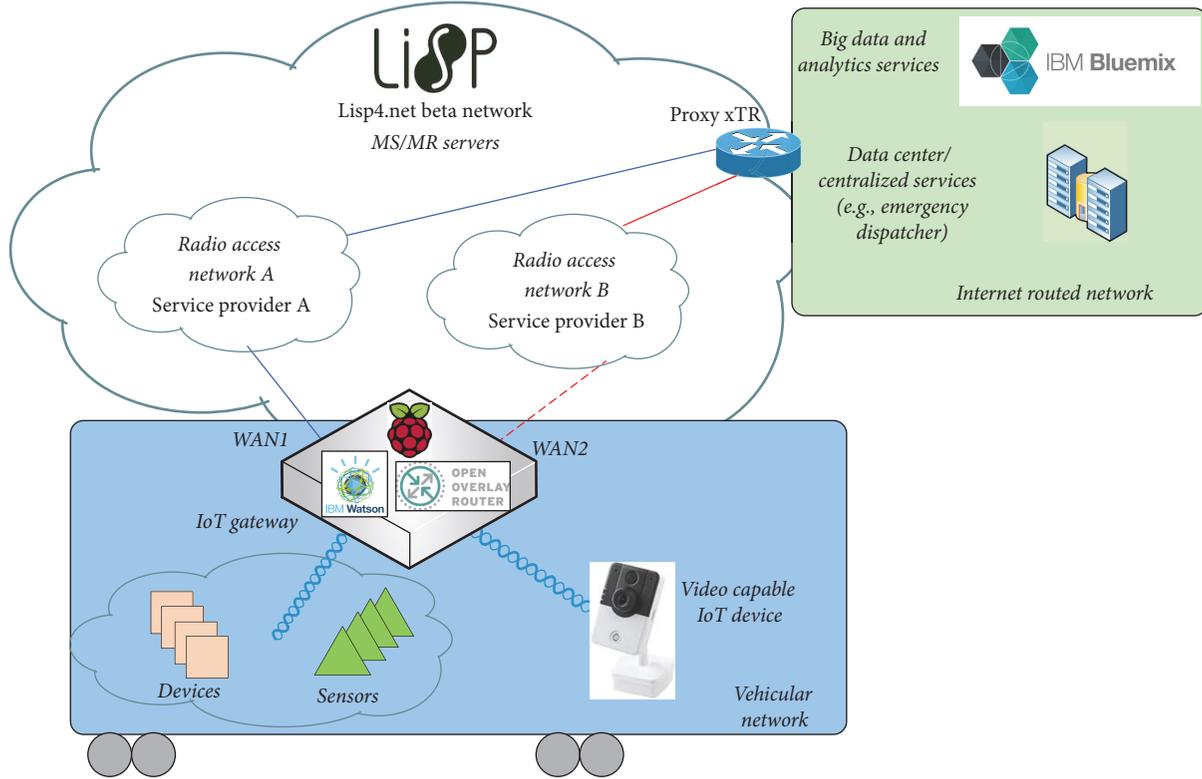


FIGURE 2: Simple prototyping of in-vehicle LISP configuration for IoT, based on open solutions (OOR).

In November 2016, a standard proposal was defined with the IETF LISP Working Group. This memo specifies LISP-SEC, a set of security mechanisms that provides origin authentication, integrity, and antireplay protection to LISP’s EID-to-RLOC mapping data conveyed via mapping lookup process. LISP-SEC also enables verification of authorization on EID-prefix claims in Map-Reply messages [46].

5. LISP Implementation of RAN Multihoming and Load-Balancing for Mobile IoT

As part of our previous work we have implemented a simulated demonstrator based on Cisco devices supporting LISP [47] in order to demonstrate the benefits of LISP compared to other routing protocols but also to validate security and load-balancing solutions. The demonstrator, part of our previous work, was illustrative for the LISP configuration and functionality and can be applied for several scenarios, from distributed enterprise offices to the mobility use-cases, ensuring encrypted communications, failover mechanisms, and load-balancing in an emulated enterprise environment.

Compared to the emulated demonstrator we now extrapolate to a mobility scenario. In this section, we propose an adapted mobile IoT architecture detailing the LISP elements implementation. We have considered the case of IoT elements inside a vehicular or public transportation network.

There are 2 methods that can be chosen for implementation of LISP for IoT:

- (i) On the IoT gateway that is also a multi-RAN router, as detailed in Figure 2
- (ii) Directly on the IoT element (“thing”) using the LISP-MN (Mobile Node) version of the protocol implementation.

Our proposal for an in-vehicle architecture is based on an open-source implementation. There are several open LISP implementations, and we can mention OpenLISP [48] as one of them, but we have focused our attention to Open Overlay Router, initially named LISPmob. OOR is an open-source implementation to create programmable overlay networks, written in C, offering the big advantage of platform flexibility, as there are dedicated versions for Linux, Android, and OpenWRT.

We have chosen to use the Linux OOR implementation, installed on a Raspberry Pi SBC (Single Board Computer) element that plays the role of an IoT gateway as it runs also IBM Watson [10] for “RasPi” and can also be connected to the IBM Bluemix Cloud for further analytics and processing.

Our IoT gateway implementation is illustrative for an ecosystem of overlay networks, as OOR can be integrated with the concept of Software Defined Networks [49], LISP having support also from OpenDaylight SDN Controller [50] as part of the LISPFlowMappings module [51], one of the most developed open solutions of this type. OpenDaylight can play the role of the mapping servers (MS/MR); thus decisions for the intelligent routing are collocated with the LISP mapping

Unitbv xTR	intouch-ams-mr-ms-1	Yes	Yes	00:10:00	0	153.16.61.32/28	109.166.171.20 (up) 213.233.72.16 (up)
Unitbv xTR	tdc-mr-ms	Yes	Yes	00:10:00	0	153.16.61.32/28	109.166.171.20 (up) 213.233.72.16 (up)
Unitbv xTR	upc-mr-ms	Yes	Yes	00:10:00	0	153.16.61.32/28	109.166.171.20 (up) 213.233.72.16 (up)

FIGURE 3: LISP4. Beta implementation for our “Unitbv” xTR nodes.

servers. Furthermore, SDN controllers play a crucial role in the concept of network slicing defined for Network Functions Virtualization [52] environments in 5G networks, and one dedicated mobile operator network slice can be exactly the IoT slice.

There are more roles that are implemented as part of the OOR open solution: currently, it can operate as an xTR, MS/MR, RTR, or LISP-MN. We have enabled LISP on the WAN router that acts as xTR. Another scenario could have been the usage of LISP-MN directly on the Android phone, as depicted in Figure 1.

Furthermore, the IoT gateway element has 2 mobile WAN interfaces for two local mobile operators that we will further name Operator 1 and Operator 2. In order not to give any benchmarking details on the public mobile networks without the operator’s consent, we will not mention the commercial name of the public networks used.

The connection was possible via 3G USB modems and the Linux tool wvdial. Each of the interfaces has a public RLOC address as visible in Figure 3 on the experimental network used. For the tests performed we have chosen to use the public LISP4 pilot network [53] that has been deployed worldwide, consisting of 8 mapping servers and several proxy-xTR covering three main regions, USA, Europe, and Asia [54]. The LISP4 Beta network has an increased network of public xTR sites.

For the LISP4 Beta network usage we had to provide public/routable IP addresses in the networks of Operator 1 and Operator 2, as visible in Figure 3.

Illustration of the two point-to-point connection interfaces, each for one mobile operator, that are aggregated in the LISP tunnel interface (lispTun0), based on the Open Overlay Router implementation, is shown in Box 1.

6. IoT Video Analytics

Wireless video traffic is expected to be 60–75% of the global mobile traffic by 2020 according to Cisco [55], but this percentage will increase considering the new set of applications to be launched in the “everything connected” Internet of Things upcoming era. Internet of Multimedia Things (IoMT) represents the proliferation of real-time communication services that involve the interaction of smart heterogeneous multimedia things with one another and with other Internet connected elements [3].

That is the reason why we have decided that in order to reveal the benefits of multihoming the Internet of Multimedia Things use-case is relevant, as this type of applications is very

demanding from bandwidth and processing power point of view.

Some scenarios for IoT based on multimedia communication are as follows:

- (i) Coupled with video analytics, the use-case also chosen by us for implementation (e.g., face/object recognition, behavior interpretation, automatic alerts when movement of objects is inconsistent with predefined patterns, and smart business management and marketing)
- (ii) Browser-based creation of ad hoc video rooms or audio calls that could aggregate the scenario requested resources (e.g., ambient assisted living, communication with ad hoc medical personal, or including artificial intelligence)
- (iii) Video based robot/UAV controlling (e.g., “see what I see” scenarios).

For some of the above-mentioned services, the video quality [56] becomes essential in the case of Critical Communications. For example, video analytics could be used in a restricted area (like an oil plant) to monitor the mobile workforce and signal when employees are in a dangerous situation (“man down” scenario).

That is why when involving mobility and video analytics there is a need to ensure the system reliability and a good image quality, so the video processing is effective. The adaptive codecs are reducing the video quality in case of bandwidth reduction, but this could deteriorate the video to the limit, thus becoming improper for analysis. Solutions for multihoming and load-balancing could become effective in keeping the available bandwidth high; thus the automatic quality adaptations of modern codecs in case of poor network conditions will not affect the video analysis.

From our implementation point of view we have chosen to use IBM Watson and IBM Bluemix for the IoT and video analytics components. One of the reasons for choosing Watson is that it can be installed on Linux based systems like the Raspbian operating system, so it can cope with our Open Overlay Router implementation. Furthermore, it offers the distributed processing power of IBM Bluemix from the Cloud. With Watson, one can analyze and interpret all the IoT data, including unstructured text, images, audio, and video.

We have used NodeRED [57] for IoT service description and, as part of our basic video analytics and for demonstrative purposes, we have considered the simple case of facial recognition. Figure 4 illustrates the image processing chain

```

lispTun0    Link encap: UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
            UP POINTOPOINT RUNNING MTU: 1440 Metric: 1

ppp0       Lin encap: Point-to-Point Protocol
            inet addr: 109.166.171.20 P-t-P: 10.64.64.64 Mask: 255.255.255.255
            UP POINTOPOINT RUNNING NOARP MULTICAST MTU: 1500 Metric: 1

ppp1       Lin encap: Point-to-Point Protocol
            inet addr: 213.233.72.16 P-t-P: 10.64.64.65 Mask: 255.255.255.255
            UP POINTOPOINT RUNNING NOARP MULTICAST MTU: 1500 Metric: 1
    
```

Box 1

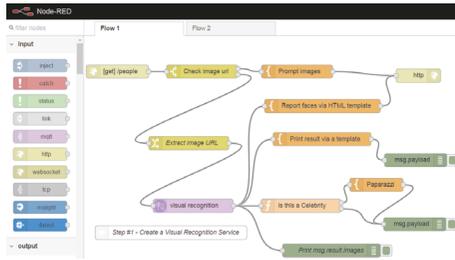


FIGURE 4: Video analytics with IBM Watson: services visually described using NodeRed.

implemented using NodeRED. For the face recognition, we considered the case of Edge Processing on the “RasPi” device with a local OpenCV (Open Computer Vision) implementation, but also the Cloud processing with Bluemix. The details of these implementations that we have realized are not scope of this paper but are illustrations on possible usage scenario with intensive bandwidth consuming applications.

7. Experimental Results for Multihoming and Load-Balancing in Mobile IoT Methodology and Testing Approach

Our testing approach is based on several steps that will be further detailed in this section:

- (i) As the multihoming and load-balancing are dependent on the mobile operator coverage maps, our first intention was to establish a baseline for the radio coverage using professional tools (e.g., the PCTEL mobile network radio scanner).
- (ii) Using this method, we have found out that not both operators investigated have proper mobile radio coverage in all areas and sometimes the loss of signals leads to interface disconnections in our demonstrator. Thus, we have decided to introduce an automation methodology to make the system more responsive in case of errors, also enhancing the LISP advantages of tunneling, independent of the number of underlying connections.
- (iii) Third step was the effective testing of video streaming methodologies that are becoming part of the IoT world. This is an innovative approach as WebRTC [58]

has not so far been extensively used for Internet of Multimedia Things. Our initial focus was based on the video quality testing, using a reference video to be played via WebRTC streams. By comparing the effective bandwidth with the video quality delivered over the network, we have discovered that mobile operators produce their own video processing/transcoding that affects the video quality.

- (iv) As the network and the WebRTC server were introducing some nonpredictive variable in our testing in relation to the effective quality of the video, we focused on the quality of experience for parallel usage of multiple WebRTC streams, where the LISP multihoming brings advantage.

7.1. *The Reference Mobile Coverage Maps.* In order to avoid our complex testing being influenced by the coverage problems of the mobile network operators, we conducted a preliminary analysis of the 3G and LTE coverage maps for the two operators used in parallel during our tests.

We have used the following mobile configuration: a “PCTEL” scanner (produced by RF Solutions), an omnidirectional antenna, and a “TEMS Investigation” software package running on a notebook (with a hardware configuration specific for Drive-Tests). The PCTEL scanner (Figure 5) enables performance assessment and offers optimizing solutions adapted to the wireless network under test (130 MHz to 6 GHz). Data are acquired in a SeeGull MX concurrent collection, for all RF bands defined by 3GPP, for all major technologies simultaneously (after a unique radio module, there are high-performance signal processing modules running in parallel).

The scanned data was analyzed using TEMS Investigation, an active end-to-end testing solution for verification and heterogeneous RAN optimization, allowing operators to test and assess the network quality from a user perspective, including in-vehicle mobility scenarios.

The first step for setting the configuration of the scanned networks is the channel and frequency bearer parameters selection (Figure 7), for the evaluated mobile operators. We have chosen the central bearer frequency for the 3G and 4G technologies and the bandwidth, specific for each ISP. The bandwidth for 3G is in general 5 MHz, while the 4G bandwidth varies between 5 MHz and 20 MHz, depending on the resource allocation for the frequencies of each operator, according to the radio licenses they are allowed to operate.



FIGURE 5: The RF Solutions “PCTEL” scanner.

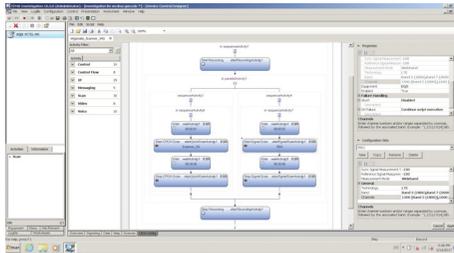


FIGURE 6: Testing configuration using visual programming with “Pctell MX SeeGull scanner.”

In Figure 6 it is presented, in a graphical format, the configuration script for the “Pctell MX SeeGull” scanner, using the TEMS Investigator software. This configuration is used for scanning the downlink service capability in 3G and 4G for the two chosen operators.

For the drive-test run we have used an application for the real-time processing of data, including also a graphical representation for some of the parameters. Thus, any error or abnormal functionality of the system could be immediately identified and corrected, so the scanning test could continue normally.

We have chosen a predefined route in the city of Brasov for the drive-test reference route. The antennas were placed on the car roof to avoid signal loss; the distance between the antennas and the car roof end should be bigger than $\lambda/2$.

While running the test we can identify the radio conditions on that specific route for each of the two operators and also get a statistic of the best channel to be used by the mobile device while performing the service. The LISP demonstrator was driven following the circuit of Figure 8; for the validation of handover correctness, the PCTEL scanned the quality of the downlink for the Operator 1 and Operator 2 cells with the EARFCN (EUTRA Absolute Radio-Frequency Channel Number) cell identities 1300 and 6250 (Operator 1) and 1600 and 2950 (Operator 2).

Not all testing results will be detailed in this paper, but using the radio scanning method we have found out that not both operators have a proper mobile radio coverage in all the parts of the reference drive-test route. There are areas where we have loss of signal for one of the operators and this leads to errors in the behavior of our LISP based IoT gateway, as a

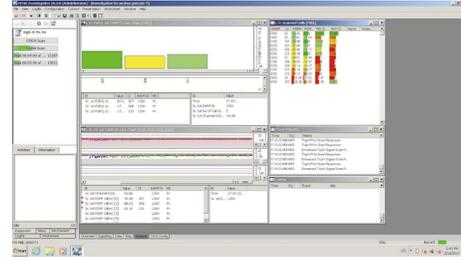


FIGURE 7: Setting the LTE central frequencies in TEMS Investigation.



FIGURE 8: Drive-test route showing the preferred channel numbers: EARFCN (EUTRA Absolute Radio-Frequency Channel Number).

disconnected mobile interface does not recover by itself and is not used again in the LISP OOR tunnel without a specific reinitiation.

Thus, we have decided to introduce, via scripting, a method for “self-healing” of the system, thus making it robust and error resistant.

7.2. Automation of the LISP-Based Mobile Demonstrator for IoMT. For the concepts presented in Section 5, we have accomplished the following demonstrator (Figure 9) that was tested in the mobility scenario.

There were considered intensive bandwidth consumers, video streams (on the screen of the end-user, a “thin client,” e.g., a tablet connected to the LISP “RasPi” node, the IoT gateway). The structure of the implemented mobile test system is given in Figure 10. Our mobile IoT demonstrator, based on LISP, is an autonomous system, battery powered, so completely mobile. All the end-users or IoT sensors and devices are automatically connected to the system via WiFi as connecting to a normal hot-spot.

System automation for treating of errors or for loss-of-signal recovery was done with bash scripting. LISP brings an additional advantage for the system robustness, besides the multihoming and load-balancing: as with the Mobile IP protocol, with LISP the TCP-IP connections are preserved no matter the availability of physical channels/connections, but with the advantage that there are less modifications needed for the network infrastructure. With our implemented scripting, besides keeping the tunnel up (and the TCP-IP

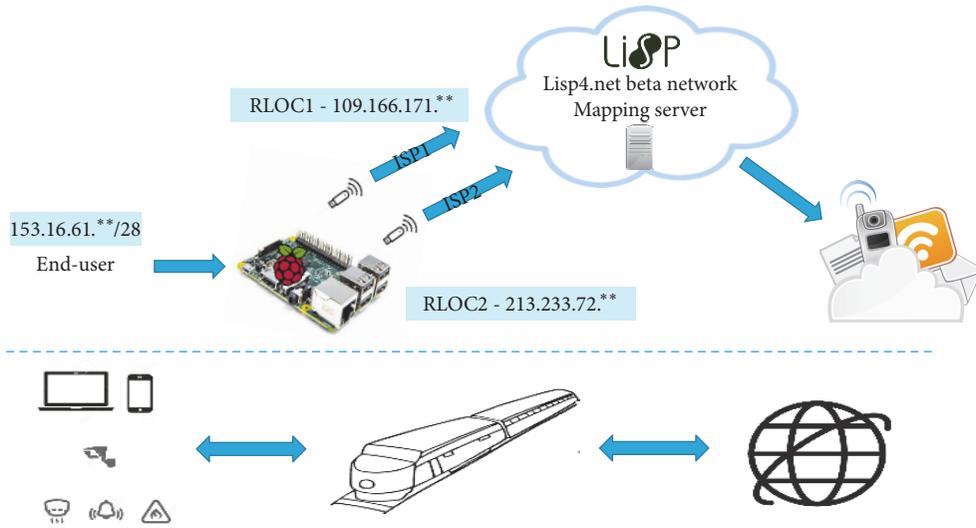


FIGURE 9: PTS (public transportation system) demonstrator for mobile IoT with LISP.

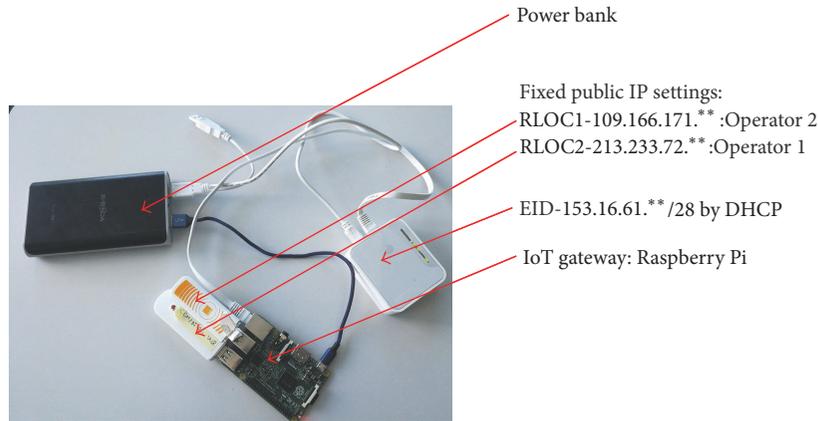


FIGURE 10: The mobile test minisystem.

connection) that is a LISP attribute we also automate a method for an interface recovery. Additionally, as emphasized in Section 3, LISP brings the advantage of a facile end-to-end implementation, as the mobile node does not necessarily need a specific implementation if it only uses LISP networks or LISP proxies.

Below there are some details of the implementation that are automated as part of the “self-healing” script. The network access for the two mobile operators (based on the AT commands for GPRS, CG, to set up the APN and the extended quality of service required) can be configured with any software tool as in the following example (for *wvdial* tool):

See Boxes 2 and 3.

The OOR (Open Overlay Router) was configured with two router interfaces and three MS (Map Servers), according to the addressing space allocated in Figure 3.

See Boxes 4 and 5.

Here there are some scripting extracts for the interfaces startup and routing configuration.

See Box 6.

```
[Dialer Operator 1]
Init1 = ATZ
Init2 = AT + CGDCONT = 1, "IP", "ipfix.operator1.ro"
Init3 = at + cgeqreq = 1, 2, 0, 0, 0, 0, 2, 0, "0E0", "0E0", 3, 0, 0
Stupid Mode = 1
Modem Type = Analog Modem
Phone = *99 * * * 1#
Modem = /dev/ttyUSB3
Username = { }
Password = { }
Baud = 460800
```

Box 2

It is important to mention that although all OOR configurations were properly realized, the routes on the IoT gateway device were not set as part of the OOR deployment for multihoming support.

```
[Dialer Operator 2]
Init1 = ATZ
Init2 = AT + CGDCONT = 1, "IP", "lant"
Init3 = at + cgeqreq = 1, 2, 0, 0, 0, 2, 0, "0E0", "0E0", 3, 0, 0
Stupid Mode = 1
Modem Type = Analog Modem
Phone = *99 * * * 1#
Modem = /dev/ttyUSB0
Username = {}
Password = {}
```

Box 3

```
rtr-ifaces {
  rtr-iface {
    iface = ppp0
    ip_version = 4
    priority = 100
    weight = 50
  }
  rtr-iface {
    iface = ppp1
    ip_version = 4
    priority = 100
    weight = 50
  }
}
```

Box 4

Typically, a host connected to a network, such as the Internet, will have one default route using a WAN interface. However, if a second WAN interface is added and both are accessed, one can end up with a situation referred to as “(hot) potato routing,” or deflection routing, meaning the answer to some request coming over the second WAN interface will be replied using only the first WAN interface that is considered the default route. Thus, we had to manually configure two default gateways by setting two lookup rules with the same priority, 1000 in our case, ensuring that the two redundant multihomed paths are used in parallel.

7.3. WebRTC as Video Streaming over LISP Network. For testing purpose, our focus was to use the latest web technologies. When it comes to Real-Time Communications, WebRTC is the new standard, enabling browsers and mobile applications with Real-Time Communications (RTC) capabilities via simple APIs (Application Programming Interfaces).

Being purely browser based and not requesting any application or plug-in installation [59, 60] make WebRTC a versatile option that could easily be accommodated and embedded as part of the heterogeneous IoT ecosystem.

Even if there are several open tools dedicated for WebRTC [61] signaling testing, mostly focused on functional and load testing of WebRTC signaling (e.g., Telestax/Restcomm implementation [61]), emulating connection of hundreds or

```
map-server {
  address = 147.83.131.32
  key-type = 1
  key = 6YAuVd8BRJ
  proxy-reply = off
}
map-server {
  address = 193.162.145.50
  key-type = 1
  key = 6YAuVd8BRJ
  proxy-reply = off
}
map-server {
  address = 217.8.98.42
  key-type = 1
  key = 6YAuVd8BRJ
  proxy-reply = off
}
```

Box 5

thousands of simultaneous clients, there are few options in regard to testing the quality of the video streams, once the signaling is established [62]. Of course, we must mention the professional testing tools, used by mobile operators for optimizing their network, like TEMS [63] or Nemo Outdoor [64].

For the video quality testing there are also some implementations like CodeUrjc [65], but this requires also the installation of a Kurento Media Server and a complex setup methodology to perform the tests, difficult to be used with public WebRTC servers.

As we were interested to also assess the quality of the video streams, we have designed our own WebRTC testing procedure. For IoMT the quality of the video can be critical, so below some minimum quality threshold the video processing cannot be considered relevant.

Using a webcam driver, we have simulated a video source and we were able to broadcast a known/reference video into a WebRTC stream. We have used public available WebRTC servers like OpenTok [66] and AppRTC [67] to produce WebRTC video conferences.

Even not depicted in the following (Figure 11), several WebRTC streams were simulated. On the corresponding edge, we have recorded the video stream using the RecordRTC tool [68]. Thus, once broadcasted via the WebRTC system, the reference video stream is recorded and can be analyzed at the corresponding edge.

7.3.1. Testing Solutions. Once the WebRTC streams were captured using the above-mentioned methodology, for the comparative quality estimation of video streams we used the tool named qpsnr [69]. It measures the peak signal-to-noise ratio (PSNR) and the structural similarity index (SSIM). SSIM is a method for predicting the perceived quality of digital television and cinematic pictures, as well as other kinds of digital images and videos. SSIM is basically used for measuring the similarity between two images and it is designed to improve on traditional benchmarks such as

```

...
if [ -z "ifconfig | grep 'ppp1'"];
then
{
sleep 15
sudo ifconfig eth0 down
sudo ip route add default dev ppp0 table multihome_operator 2
sudo ip rule add from 109.166.171.20 lookup multihome_operator 2 prio 1000
sudo ifconfig eth0 up
}
...

```

Box 6

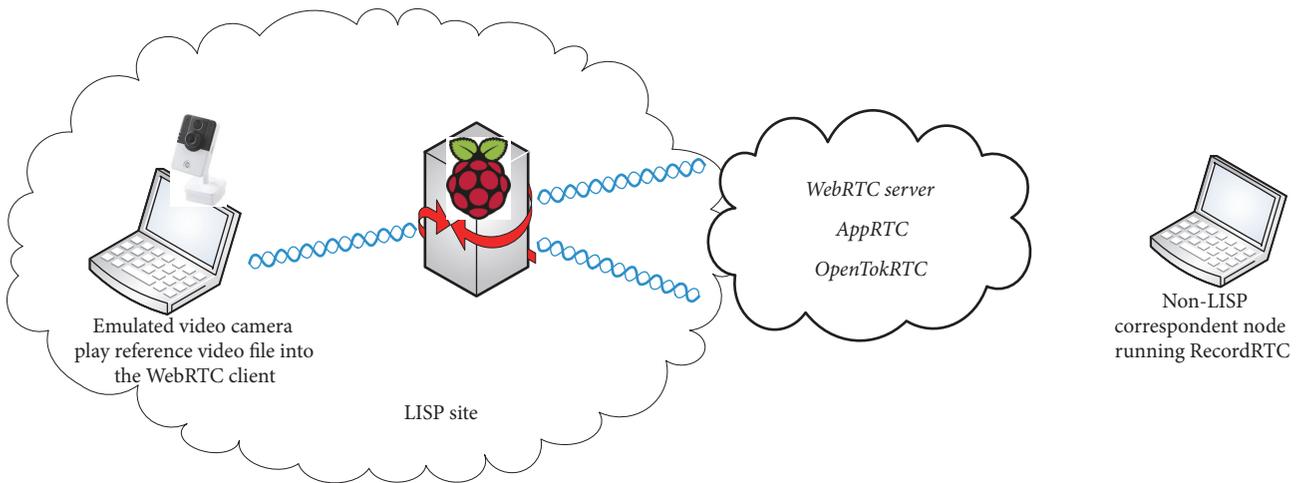


FIGURE 11: Method for testing WebRTC streams.

PSNR and mean squared error (MSE), which have proven to be inconsistent with human visual perception.

The second test that we have performed uses an older IIS Microsoft feature for Live Streaming called Smooth Streaming [70]. It is based on an IIS7 feature called IIS Media Services that makes it possible for the server to understand the live video player requests and timecode.

This Live Smooth Streaming IIS feature was previously used by Content Delivery Network (CDN) providers like Nimbus, Edgecast, or Akamai that are also currently major Cloud CDN providers. When IIS was used, the Smooth Streaming was performed based on the codec named Expression Encoder 4 Pro or with hardware encoders, but now the CDN providers are supporting the latest streaming formats such MPEG-DASH for live delivery.

The HTTP-based Smooth Streaming infrastructure requests for little video chunks from the broadcasting web server. The web server looks up the correct video “chunk” within the audio/video file and serves it up. The Smooth Streaming Performance Testing Tool (Figure 12) emulates a Smooth Streaming player that makes tiny HTTP requests requesting a second or two of video at a certain bitrate (e.g., “give me 230 k @ 00:01:06, give me 708 k @ 00:01:08”). Requesting different quality video chunks and evaluating the response time were a method to assure the “smooth” streaming, and based on the response time for each chunk, the



FIGURE 12: Smooth Streaming Performance Testing Tool, performing video quality requests and evaluation of the response time.

encoding bitrates are switched and adjusted to the network connection capability.

So even if it is not a real streaming test, this method is a good indicator of the network connection capability and the most proper bitrate for a video to be transmitted over a certain connection. For our tests we have used a streaming server, now part of the Akamai network [71].

7.3.2. Test Results and Analysis of Video Quality. By using the qpsrn tool comparative testing for video quality we have observed that Operator 1 video quality is lower compared to Operator 2 and to multihoming dual use of Operator 1 + Operator 2.

However, other bandwidth tests, like, for example, “classical” bandwidth online testers (like Speedtest [72]), indicated that Operator 1 has actually a better throughput. With our

testing we were able to prove that Operator 1 has in place the so-called Mobile Video Optimization (MVO) technique that covers the use of technologies and solutions enabling the mobile network operators to optimize the delivery of video content through video optimization techniques, prioritization policies, user-based customization, and intelligent management of overall traffic on their data networks.

Besides MVO, there are other elements to be taken into consideration that have a great influence on the one-to-one comparative video quality analyses using qpsrn:

- (i) *Local browser codec*. The played video (from the video source, the webcam, or in our case the emulated webcam), is further processed by the browser as part of the WebRTC stream. In this case, the browser supported code is essential, as some video codecs are adapted for multiple connections, such as H.264 SRE and H.265 with their “Google correspondents” VP8 and VP9. VP8 is a highly efficient video compression technology developed by the WebM Project. For most of the browsers, the default audio codec is OPUS while for video codec it is VP8. VP9, with better features related to multipath streaming, has no “native” support in Chrome, so in order to enable it, the Chrome browser should be started with the command “chrome.exe –enable-webrtc-vp9-support”
- (ii) *The media mode of the webRTC implementation (relayed or routed)*. When establishing a WebRTC connection, at session creation it is specified how clients in the session will send audio-video streams, known as the media mode with two options STUN and/or TURN. The “relay server” is a TURN server. If both options are available, web browser will start trying to use STUN first. However, if clients cannot connect due to firewall restrictions or NAT, the session uses the TURN server to relay audio-video streams (also the case for the OpenTok WebRTC implementation that we have used). WebRTC should be transferring peer-to-peer data, once signaling is established, but using TURN mode in OpenTok introduces another point for multimedia transcoding and stream optimization.

Thus, we have concluded that an accurate video analysis test for comparing a LISP multihomed network to other network needs some enhancements to our testing methodology:

- (i) Use local MS/MS servers, as the Proxy LISP server used as part of the LISP4 Beta network is introducing delays as they are not optimally placed.
- (ii) Use a local WebRTC STUN server; avoid NAT and other proxies.
- (iii) Preset the same codec to be used, or even force a “non-bandwidth-adaptive” codec, so that bandwidth is reflected in the video quality and can be analyzed with tools like qpsrn.

Another conclusion was that we should focus on the quality of experience delivered, as the variables introduced

by the infrastructure elements (the media server and the network operator video processing) are not controllable. Also, we focused on the LISP advantages for multihoming that are visible in case the network resources are scarce, like in the scenario of using multiple parallel video streams (see Section 7.3.3).

For evaluating the traffic throughput, as visible in Table 1, we have used the iptraf-ng tool.

However, while the previous LISP multihoming results [22] show that the weighted load-balancing is respecting the weight percentages set for each redundant LISP link (since a lot of small files were transferred as part of the BitTorrent transfer), in a continuous data stream the load-balancing between the two WAN connections is not respecting the OOR preconfigured weights. The reason is the source based routing used, which has the effect of routing the packets towards a certain destination based on the source IP address. So the effect is that if we use only one connection towards a server (one video stream), those packets will be routed preferably over one link. In the case of BitTorrent, we have a lot of small connections with a lot of destination IP addresses, which explains the even distribution of the traffic.

Also for the bandwidth tests we have observed, in the results of the Smooth Stream Performance testing, that LISP multihoming is not efficient in case of successive requests and intensive signaling (see Figure 8) like in the case of retrieving different streaming chunks based on a manifest. For each type of streaming (audio/video), the bitrate is mentioned, as well as the response.

The results in Table 1 do not indicate an improvement by using two parallel WAN connections, as none of the mobile connections was lacking bandwidth; there was no bottleneck even if the excessive signaling of using two parallel connections caused its own delay.

7.3.3. Quality of Experience for Multiple WebRTC Streams over LISP Tunneling. In this way, we have tried to use multiple multimedia streams, like in a real case where multiple IoMT devices are connected to the same IoT gateway and focus on quality of experience. For testing purpose, we have connected several WebRTC streams to the same conference using the same OpenTok WebRTC implementation.

We have observed that, at each WebRTC connection establishment, the traffic was directed either to Operator 1 or to Operator 2. The load-balancing observed was not for splitting the video stream over two WAN mobile connections, but in the distribution of video streams on different of data paths.

To better explain the situation, we could make an analogy with the multicore processors: when only a thread is running (in our case one WebRTC session), just one core is used (in our case mostly one operator network is used); in case a second thread is starting, it is taken over by the second core processor (in our case the Operator 2), thus balancing the traffic between the 2 operators. This behavior is visible in the bandwidth monitoring results (see Figure 14). When only one WebRTC stream is started, only one operator network is used; then the second stream is started and this is taken over mostly by operator 2.

TABLE 1: Load-balancing with multiple WebRTC streams performed as observed with Linux tool iptraf-ng.

Iface	iptraf-ng 1.1.4					
	Total	IPv4	IPv6	NonIP	BadIP	Activity
lo	152	152	0	0	0	0.00 kbps
eth0	377005	376934	71	0	0	3012.05 kbps
wwan0	34	32	2	0	0	0.00 kbps
wwan1	34	32	2	0	0	0.00 kbps
ppp0	230081	230081	0	0	0	1170.34 kbps
ppp1	155369	155369	0	0	0	2056.27 kbps
lispTun0	377582	377582	0	0	0	3012.14 kbps

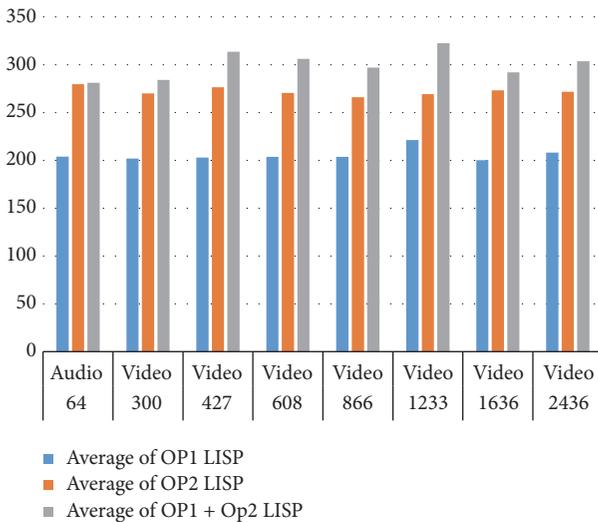


FIGURE 13: Smooth Streaming Performance Testing comparative results between Operator 1, Operator 2, and multihomed Operator 1 + Operator 2 tests. The figure indicates the response time (in ms) to retrieve different stream chunks from a remote streaming server.

The results in Figures 13 and 14 indicate that benefits of using two or more mobile connections are mostly visible in case of multimedia information when using multiple video streams and when congestion is affecting the network.

Furthermore, our intention was to limit the bandwidth of the mobile connections, so we can better assess the multihoming benefits. This was performed using the AT command “AT + CGEQREQ,” with the intention to limit each network operator bandwidth to 384 Kbps. However, the mentioned command had no effect on the live operator networks that we have used, so the bandwidth was not limited in order to simulate congestion. The trend is to move the focus of the data transmission in the mobile networks from quality of service to better throughput. This explains the lack of effect of the QoS commands used.

We have concluded that, in the specific case of WebRTC, LISP usage for multihoming brings benefits for maintaining the sessions by the use of the LISP tunneling that keeps the TCP connections open with the help of the implemented automation method for interface recovery in case of loss of signal. Furthermore, the load-balancing brings significant

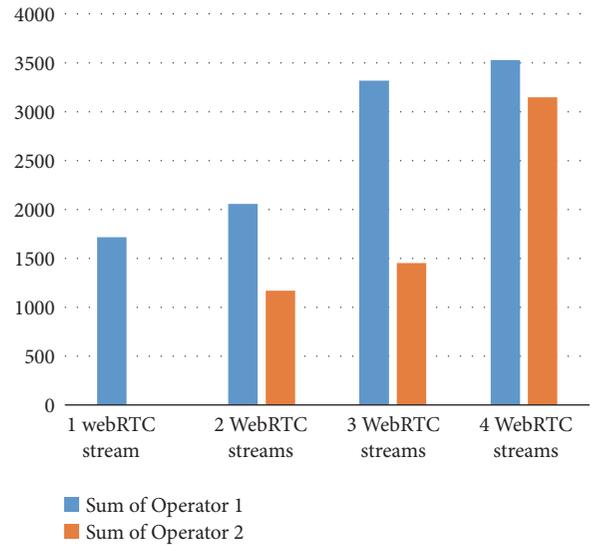


FIGURE 14: Tests indicate the bandwidth provided for each mobile operator when playing up to 4 WebRTC streams using OpenTok.

advantages when it comes to using several parallel WebRTC streams, a valid use-case for using more video capable devices attached to the same LISP-based IoT gateway.

8. Conclusions and Future Work

This paper is focused on the implementation and analysis of a multihomed and load-balanced mobile IoT system with focus on one mobility technology (the LISP protocol) and on one relevant scenario for the bandwidth demanding applications: multimedia streaming and video analytics of IoMT systems.

We have made an analysis of the LISP advantages for IoT systems from four perspectives (as LISP usage in IoT was not so far assessed by the scientific community): easiness of end-to-end deployment, mobility, multihoming, and security. We have highlighted the great advantages of LISP for mobility that can act as host/device mobility and as Virtual Machine Mobility VMM solution, so it can be a great solution for Edge Cloud processing mobility that follows the mobility of the IoT device/gateway.

Furthermore, we have implemented a demonstrator for an IoT gateway that has the role of the mobility access gateway and also it runs the IoT framework IBM Watson

with video/image analytics capability. Our demonstrator was mostly based on open solutions, using a Raspberry Pi from the hardware point of view, running the Open Overlay Router open LISP implementation and IBM Watson.

Compared to previous works and multihoming tests for LISP, we were focused on video streaming testing as part of an IoMT system and mobility. Multihoming was represented by the usage of multiple mobile operator networks simultaneously. As a baseline for our mobility testing, and to increase our tests' relevance, we have introduced a complex demonstrator of mobile IoMT validated by a reference coverage scanning with high-tech industrial radio equipment and professional dedicated software.

The robustness of the system was ensured by a new automated treatment of radio coverage gaps: the session-oriented solution due to the LISP-EID tunnel persistence was enhanced with scripting for the automatic recovery of the system in case of failure or loss of signal.

As it is the latest technology in regard to multimedia conferencing, we have focused our test on WebRTC implementations, an innovative proposal to be used as part of IoMT systems. We have implemented our own WebRTC quality testing methodology using a webcam emulator, a recording tool, and public WebRTC servers. The experimental LISP network used for tests was the LISP4 Beta network.

In our analysis, we have presented the multiple implications and specificity of mobile multimedia testing; thus we have concluded in a set of measures that we will implement in the future for a more accurate measurement of the LISP multihoming performance: local LISP MS/MR routers, use of STUN WebRTC servers, and use of several video codecs to check the impact of adaptive bitrate streaming to the test methodology.

Furthermore, as the testing environment cannot be fully controlled (end-to-end), we have focused on the quality of experience rather than on the absolute video quality evaluation. From our tests we have presented the advantages of having multiple parallel mobile connections for the LISP multihoming and load-balancing purpose that becomes relevant when using several multimedia WebRTC streams simultaneously.

As further work, we would like to combine the current implemented IoT video analytics with the Edge Processing options, Raspberry Pi being a perfect candidate to execute some of this processing (e.g., face recognition) while further Cloud video analysis could be triggered only when additional video processing is needed. Being closer to end-user sites results in reduced transmission costs for businesses and improved quality of service for consumers. We would like to couple the LISP mobility with the Edge Processing; thus when a LISP device (having one EID) migrates from one IoT gateway (RLOC) to another, also the Edge Processing function would migrate from one IoT gateway to another. Decentralized computing mitigates the risk of a bottleneck effect when moving large amounts of data, translating into lower risk of latency and faster access for customers.

Another scenario that we want to test is to use a P2P-TV system for the video streaming tests, which uses WebRTC over P2P networks to improve the load-balancing over

the network links. Nevertheless, the lack of standardization makes such testing not fully relevant for the moment [73, 74].

One important enhancement for our work would be the usage of other types of identifiers for the EID addressing, except IPv4 or IPv6 addresses (for this, we aim to modify the Open Overlay Router implementation), that could bring advantages for the easiness of "IP-less" network addressing in Internet of Things, an important unexploited advantage of LISP mappings.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

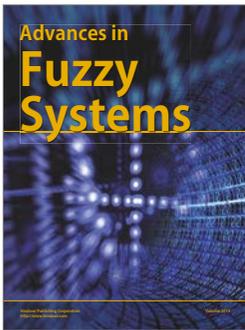
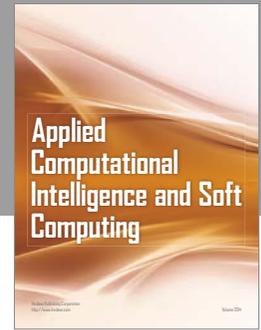
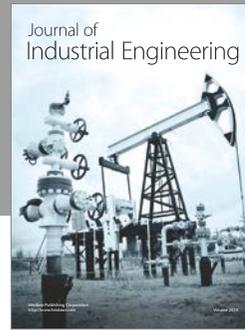
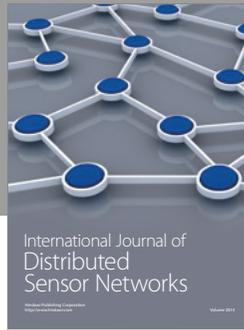
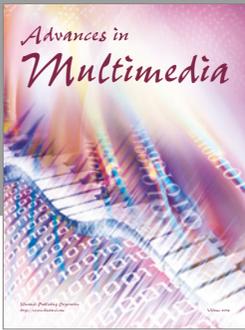
This work was partially supported by Siemens Convergence Creators SRL, Romania, who provided testing support and expertise that assisted the research. The authors thank the members of the COST Action CA15104 IRACON, "Inclusive Radio Communication Networks for 5G and Beyond," for their valuable advice and guidance related to the concepts presented in this paper.

References

- [1] NB-IOT-feature list, *Release 13 (LTE Advanced Pro)*, 3GPP, http://www.3gpp.org/images/PDF/R13_IOT_rev3.pdf.
- [2] O. Vermesan and P. Friess, *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*, River Publishers, Denmark, 2013.
- [3] S. A. Alvi, B. Afzal, G. A. Shah, L. Atzori, and W. Mahmood, "Internet of multimedia things: vision and challenges," *Ad Hoc Networks*, vol. 33, pp. 87–111, 2015.
- [4] M. J. Peltola, A. University, and H. Hammainen, "Economic feasibility of mobile broadband network for public safety and security," in *Proceedings of the 11th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, WiMob 2015*, pp. 67–74, are, October 2015.
- [5] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "The Locator/ID Separation Protocol (LISP)," RFC Editor RFC6830, 2013.
- [6] W. Ramirez, X. Masip-Bruin, M. Yannuzzi, R. Serral-Gracia, A. Martinez, and M. S. Siddiqui, "A survey and taxonomy of ID/Locator Split Architectures," *Computer Networks*, vol. 60, pp. 13–33, 2014.
- [7] "Mobile Edge Computing (MEC); Service Scenarios," in *ETSI Group Specification*, 2015, http://www.etsi.org/deliver/etsi_gs/MEC-IEG/001.099/004/01.01.01.60/gs_MEC-IEG004v010101p.pdf.
- [8] T. Taleb and A. Ksentini, "Follow Me cloud: interworking federated clouds and distributed mobile networks," *IEEE Network*, vol. 27, no. 5, pp. 12–19, 2013.
- [9] "Open Overlay Router (OOR)," <http://www.openoverlayrouter.org>.
- [10] "IBM Watson," <https://www.ibm.com/watson>.
- [11] G. Dandachi, S. E. Elayoubi, T. Chahed, and N. C. Taher, "Performance evaluation of user centric multihoming strategies in LTE/WiFi networks," in *Proceedings of the 2016 IEEE Wireless Communications and Networking Conference, WCNC 2016*, qat, April 2016.

- [12] S. Mukherjee, A. Baid, I. Seskar, and D. Raychaudhuri, "Network-assisted multihoming for emerging heterogeneous wireless access scenarios," in *Proceedings of the 2014 25th IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communication, IEEE PIMRC 2014*, pp. 1520–1524, usa, September 2014.
- [13] T. Aura, P. Nikander, and G. Camarillo, "Effects of Mobility and Multihoming on Transport-Protocol Security," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, pp. 12–26, Berkeley, CA, USA, May 2004.
- [14] A. Dhraief and A. Belghith, "Multihoming support in the Internet: A state of the art," in *Proceedings of the International Conference on Models of Information and Communication Systems (MICS)*, Rabat, Morocco, 2010.
- [15] B. M. Sousa, K. Pentikousis, and M. Curado, "Multihoming Management for Future Networks," *Mobile Networks and Applications*, vol. 16, no. 4, pp. 505–517, 2011.
- [16] J. R. Iyengar, P. D. Amer, and R. R. Stewart, "Concurrent multipath transfer using SCTP multihoming over independent end-to-end paths," *IEEE/ACM Transactions on Networking*, vol. 14, no. 5, pp. 951–964, 2006.
- [17] Ł. Budzisz, R. Ferrús, A. Brunstrom et al., "Towards transport-layer mobility: Evolution of SCTP multihoming," *Computer Communications*, vol. 31, no. 5, pp. 980–998, 2008.
- [18] A. Gladisch, R. Daher, and D. Tavangarian, "Survey on mobility and multihoming in future internet," *Wireless Personal Communications*, vol. 74, no. 1, pp. 45–51, 2014.
- [19] P. Holliday, "NOMAD A Mobile Ad Hoc and Disruption Tolerant Routing Protocol for Tactical Military Networks," in *Proceedings of the 2009 29th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS Workshops)*, pp. 488–492, Montreal, Quebec, Canada, June 2009.
- [20] B. Simpson and S. N. Bhatti, "An identifier-locator approach to host multihoming," in *Proceedings of the 28th IEEE International Conference on Advanced Information Networking and Applications, IEEE AINA 2014*, pp. 139–147, can, May 2014.
- [21] A. Rodríguez Natal, L. Jakab, M. Portolés et al., "LISP-MN: mobile networking through LISP," *Wireless Personal Communications*, vol. 70, no. 1, pp. 253–266, 2013.
- [22] D. Saucez, L. Iannone, A. Cabellos, and F. Coras, "Locator/ID Separation Protocol (LISP) Impact," RFC Editor RFC7834, 2016.
- [23] S. Haeri, R. Gill, M. Hay, T. Wong, and L. Trajkovic, "Multihoming with locator/ID Separation Protocol: An experimental testbed," in *Proceedings of the 14th IFIP/IEEE International Symposium on Integrated Network Management, IM 2015*, pp. 1238–1241, can, May 2015.
- [24] D. Saucez, B. Donnet, L. Iannone, and O. Bonaventure, "Inter-domain traffic engineering in a locator/identifier separation context," in *Proceedings of the 2008 IEEE Internet Network Management Workshop, INM 2008*, usa, October 2008.
- [25] B. Haindl and M. Lindner, "Ground based lisp for multilink operation in ATN/IPS communication infrastructure," in *Proceedings of the 35th DASC Digital Avionics Systems Conference, DASC 2016*, usa, September 2016.
- [26] B. Haindl, "LISP – A Multi-Homing and Mobility Solution for ATN using IPv6," in *Proceedings of International Civil Aviation Organization (ICAO), Aeronautical Communications Panel (ACP) - 7th meeting of Working Group 1*, Montreal, CA, 2014.
- [27] T. McParland, "Multihoming in the ATN/IPS," in *Proceedings of the 2016 Integrated Communications Navigation and Surveillance (ICNS)*, pp. 2B2-1–2B2-11, Herndon, VA, USA, April 2016.
- [28] M. F. Almirall, *Wireless LISP: Prototyping and Evaluation - A LISP Implementation in the BOWL Testbed at Deutsche Telekom Labs [Master, thesis]*, Technische Universität Berlin, 2011, <https://core.ac.uk/download/pdf/41803776.pdf>.
- [29] F. Castro, A. Martins, N. Capela, and S. Sargento, "Multihoming for uplink communications in vehicular networks," in *Proceedings of the 2017 Wireless Days (WD)*, pp. 230–237, Porto, Portugal, March 2017.
- [30] M. Alexandru and R. Urechiatu, "LTE Indoor Radio Coverage Optimization Study in Modern City Environments," *Review of the Air Force Academy*, vol. 2, no. 26, 2014.
- [31] L. Stornaiuolo and P. Bellavista, "State-of-the-art multihoming solutions for Android: A quantitative evaluation and experience report," in *Proceedings of the 11th International Conference on Network and Service Management, CNSM 2015*, pp. 158–162, esp, November 2015.
- [32] S. M. Ghaleb, S. Subramaniam, Z. A. Zukarnain, and A. Muhammed, "Mobility management for IoT: a survey," *Eurasip Journal on Wireless Communications and Networking*, vol. 2016, no. 1, article 165, 2016.
- [33] LISP Overview, *Cisco Whitepaper*, <http://lisp.cisco.com/lisp-over.html>.
- [34] L. Iannone, D. Saucez, and O. Bonaventure, "Implementing the locator/ID separation protocol: design and experience," *Computer Networks*, vol. 55, no. 4, pp. 948–958, 2011.
- [35] V. Jain, *A study of Locator ID Separation Protocol*, 2011, MSc paper, Kansas-City University/ProQuest publishers.
- [36] M. Isah and C. Edwards, "Inter-domain Mobility with LISP-MN - A Performance Comparison with MIPv6," in *Proceedings of the 8th IFIP Wireless and Mobile Networking Conference, WMNC 2015*, pp. 80–87, deu, October 2015.
- [37] S.-I. Choi and S.-J. Koh, "Use of Proxy Mobile IPv6 for Mobility Management in CoAP-Based Internet-of-Things Networks," *IEEE Communications Letters*, vol. 20, no. 11, pp. 2284–2287, 2016.
- [38] C. Mavromoustakis, G. Mastorakis, and J. M. Batalla, Eds., *Internet of Things (IoT) in 5G Mobile Technologies*, Springer, ISBN, 2016.
- [39] S. Secci, P. Raad, and P. Gallard, "Linking virtual machine mobility to user mobility," *IEEE Transactions on Network and Service Management*, vol. 13, no. 4, pp. 927–940, 2016.
- [40] J. Mueller and T. Herbert, *Mobility Management for 5G Network Architectures Using Identifier-locator Addressing*, 2016, <https://tools.ietf.org/html/draft-mueller-ila-mobility-01>.
- [41] P. Rost, A. Banchs, I. Berberana et al., "Mobile network architecture evolution toward 5G," *IEEE Communications Magazine*, vol. 54, no. 5, pp. 84–91, 2016.
- [42] A. Raheem, A. Lasebae, M. Aiash, and J. Loo, "Supporting communications in the IoTs using the location/ID split protocol: A security analysis," in *Proceedings of the 2nd International Conference on Future Generation Communication Technologies, FGCT 2013*, pp. 143–147, gbr, November 2013.
- [43] A. Stanciu, M. N. Cirstea, and F. D. Moldoveanu, "Analysis and Evaluation of PUF-Based SoC Designs for Security Applications," *IEEE Transactions on Industrial Electronics*, vol. 63, no. 9, pp. 5699–5708, 2016.
- [44] M. Aiash, "A Novel Security Protocol for Resolving Addresses in the Location/ID Split Architecture," in *Network and System Security*, vol. 7873 of *Lecture Notes in Computer Science*, pp. 68–79, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

- [45] M. Aiash, A. Al-Nemrat, and D. Preston, "Securing Address Registration in Location/ID Split Protocol Using ID-Based Cryptography," in *Wired/Wireless Internet Communication*, vol. 7889 of *Lecture Notes in Computer Science*, pp. 129–139, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.
- [46] F. Maino, V. Ermagan, A. Cabellos, and D. Saucez, "LISP-Security (LISP-SEC)," <https://tools.ietf.org/html/draft-ietf-lisp-sec-12>.
- [47] T. Balan, D. Robu, and F. Sandu, "LISP Optimisation of Mobile Data Streaming in Connected Societies," *Mobile Information Systems*, vol. 2016, Article ID 9597579, 2016.
- [48] "The OpenLISP Project," <http://www.openlisp.org/>.
- [49] T. Nadeau and K. Gray, "SDN: Software Defined Networks, An Authoritative Review of Network Programmability Technologies," *O'Reilly Media*, 2013.
- [50] "OpenDaylight: Open Source SDN Platform," <https://www.opendaylight.org>.
- [51] *OpenDaylight: LISP Flow Mapping*, https://wiki.opendaylight.org/view/OpenDaylight_Lisp_Flow_Mapping:Architecture.
- [52] R. Cziva, S. Jouet, D. Stapleton, F. P. Tso, and D. P. Pezaros, "SDN-based virtual machine management for cloud data centers," *IEEE Transactions on Network and Service Management*, vol. 13, no. 2, pp. 212–225, 2016.
- [53] *The LISP pilot network*, <http://www.lisp4.net/>.
- [54] "The International LISP Beta Network," <http://www.lisp4.net/images/lisp-ddt.pdf>.
- [55] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020," http://www.cisco.com/c/dam/m/en_in/innovation/enterprise/assets/mobile-white-paper-c11-520862.pdf.
- [56] L. G. U. Garcia, E. P. L. Almeida, V. S. B. Barbosa et al., "Mission-critical mobile broadband communications in open-pit mines," *IEEE Communications Magazine*, vol. 54, no. 4, pp. 62–69, 2016.
- [57] Node-RED, "Flow-based programming for the Internet of Things," <https://nodered.org/>.
- [58] S. Loreto and S. P. Romano, "Real-Time Communication with WebRTC," *O'Reilly Media*, 2014.
- [59] M. Fadda, M. Murrioni, and V. Popescu, "Interference Issues for VANET Communications in the TVWS in Urban Environments," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 7, pp. 4952–4958, 2016.
- [60] A. Johnston and D. Burnett, *WebRTC: APIs and RTCWEB Protocols of the HTML5 Real-Time Web*, Digital Codex LLC, 2014.
- [61] WebRTC Test, *Framework for functional and Load Testing of WebRTC*, <https://github.com/RestComm/webrtc-test>.
- [62] J. Nightingale, Q. Wang, and C. Grecos, "Performance evaluation of concurrent multipath video streaming in multihomed mobile networks," *International Journal of Digital Multimedia Broadcasting*, vol. 2013, Article ID 319594, 2013.
- [63] "TEMS - Testing, monitoring, and analytics of radio and core networks," <http://www.tems.com>.
- [64] "Nemo Outdoor 5.1 mobile testing," <http://www.anite.com/businesses/networks-testing/news/nemo-outdoor-51-ready-road>.
- [65] "CodeUrjc - automated assessment of WebRTC parameters," <https://github.com/codeurjc/webrtc-benchmark>.
- [66] "TokBox WebRTC Demo on OpenTok platform," <https://opentokrtc.com>.
- [67] AppRTC, "Video-conference demo app based on WebRTC," <https://appr.tc/>.
- [68] RecordRTC, "WebRTC Audio, Video and Screen Recording," <https://www.webrtc-experiment.com/RecordRTC/>.
- [69] QPSNR, "A quick PSNR/SSIM analyzer," <https://github.com/hsanson/qpsnr>.
- [70] SSPERF, "Smooth Streaming Performance Testing Tool," <https://ssperf.codeplex.com/>.
- [71] "Akamai Live video streaming tool," <https://www.akamai.com/us/en/resources/live-video-streaming.jsp>.
- [72] "Speedtest – Global Broadband Speed Test," <http://beta.speedtest.net/>.
- [73] Streamroot DNA, "distributed delivery architecture for large-scale OTT and broadband TV," <https://www.streamroot.io>.
- [74] Peer5, "P2P CDN (peer-to-peer content delivery network)," <https://www.peer5.com/>.



Hindawi

Submit your manuscripts at
<https://www.hindawi.com>

