Hindawi Publishing Corporation
Mobile Information Systems
Volume 2016, Article ID 9597579, 14 pages
http://dx.doi.org/10.1155/2016/9597579

Hindawi

Research Article

LISP Optimisation of Mobile Data Streaming in Connected Societies

T. Balan, D. Robu, and F. Sandu

Transilvania University, Electronics and Computers Department, Bd. Eroilor nr 29A, 500036 Brasov, Romania

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

Received 5 August 2016; Accepted 6 November 2016

Academic Editor: Maurizio Murroni

Mobility mechanisms are key elements of "always connected" smart environments. Since the first mobile IPv4 protocols, the IP mobility solutions have evolved from host mobility to network mobility and migration to IPv6, but there are still use-cases to be covered, especially for redundant multihomed scenarios. Also mobility does not refer only to hosts or individuals, but also to code/applications and to virtual machines. LISP (Locator/Identifier Separation Protocol) can contribute to new solutions for both host mobility and virtual machine mobility (e.g., inside enterprise data centers) by the separation of the identifier and location of a network endpoint. The aim of this paper is to propose a LISP based multihome and load-balanced network architecture for urban environments. Validation is done in an emulated environment for the case of an enterprise with distributed locations, but, furthermore, we extrapolate to other mobile urban scenarios, like the case of providing reliable load-balanced and secured Internet in Public Transportation Systems, with a proposal for an open-source implementation.

1. Introduction

One of the research challenges for next generation all-IP-based wireless systems is the design of intelligent mobility management techniques [1] to achieve global seamless roaming, reliability, and high quality of experience for a series of services. These have an increased demand in resources, either from end users (e.g., bandwidth consuming video streaming) or from the growing number and diversity of IoT applications [2].

The mobility challenge solved by of Mobile IP (MIP), with all its variations (from MIPv4 to MIPv6, with the Hierarchical MIP, HMIP), and Fast MIP (FMIP) is now doubled by new service-generated challenges: the need for reliability and multihoming, the need not only for failover mechanisms but also for load balancing between mobile connections or technologies, and for security mechanisms in case of critical data communications. The network enhancements that should be implemented in order to support these new requirements should make a minimum impact in the existing network (wide area network, WAN) design [3, 4].

Furthermore, in the era of virtualization, mobility has received new meanings: the applications/workloads are hosted on virtual servers, so they are detached from the physical infrastructure, thus becoming mobile by definition [5, 6].

The fact that endpoints are decoupled from the physical infrastructure and can be mobile has triggered some new changes in the routing infrastructure: the topology centric addressing model, which we are used to, has to evolve to a more flexible architecture, so that endpoints could still be addressed while they are roaming across the infrastructure [7].

One of the solutions for these expressed challenges for user mobility but also for application and virtual machine mobility is considered to be the Locator/Identifier Separation Protocol, LISP [8]. The current Internet routing and addressing architecture is changed by LISP through the separation of the identifier and location of an endpoint (the "who" and "where" in networking).

Our motivation was to find a solution for transporting large amount of real-time information (e.g., video streaming), using reliable and secure connectivity, to mobile users in crowded urban areas.

The objective of our work is to validate a multihomed load-balanced and secure environment, in an emulated Cisco configuration, based on the GNS3 emulator, that can

be further applied in mobility scenarios for urban areas, with focus on public transportation systems. The important requirement of providing reliable and secure Internet is actually the base for a series of public safety applications that are moving towards broadband connection usage, replacing or accompanying critical communication technologies like TETRA (Terrestrial Trunked Radio) [9] and GSM-R (GSM for Railways) [10].

The paper is structured as follows: first section describes the LISP protocol concept and functionality, and second section describes the implemented LISP demonstrator with focus on a distributed enterprise use-case that can further be extrapolated to other domains like mobility in urban areas. Third section is focused on the description of the methods to provide Internet-based services for the public transportation system, presenting our proposed LISP based architecture for vehicular networks. Further, the paper is focused on a proposal for an open-source implementation of a vehicle network using Open Overlay Router, but with additional solution enhancements based on Software Defined Networks (SDN), with the specific case of Software Defined-Wide Area Networks (SD-WAN), including WAN optimization.

2. Locator/Identifier Separation Protocol

LISP is a network architecture and a set of "map-and-encapsulate" network-layer based protocols developed by the IETF (Internet Engineering Task Force) "LISP Working Group" in RFC 6830 [6] that documents the separation of IP addresses into two new numbering spaces: Endpoint Identifiers (EID-s) and Routing Locators (RLOC-s) [11]. By introducing this separation, new capabilities for mobility, scalability, and security become available [12]. In LISP, both identifiers and locators can be IP addresses, but also other identifiers-locators sets are accepted like, for instance, a set of MAC addresses and GPS coordinates.

The EID identifies the nodes that are connected to the network. The RLOC identifies the location; it uses the traditional addressing scheme: IPv4 and IPv6; in fact this is the public address of the routers [13].

One of the most important advantage of LISP is multihoming, as it is "embedded" in the protocol definition, providing redundancy and load-sharing.

Compared with the other mobility protocols like MIPv4 and MIPv6, LISP guarantees optimal shortest path to the moving end points and also it supports IPv4 and IPv6 in any combination for Locator and Identity (one of the possible uses being routing IPv6 traffic over older IPv4 networks). Also the protocol is scalable and transparent for both IP domain and end points on the other side. It can be also used as an overlay to extend subnets over multiple autonomous systems. If the traffic needs to be encrypted then it can be used in conjunction with GET VPN protocol.

The main drawback is that a public IP is needed (which could imply additional costs from the network operator) for each RLOC. This is an issue especially for IPv4, but not for IPv6.

LISP Mob delegates the network functions in the following way, so that the process is transparent for the users: the RLOC-s are responsible to lookup the mapping between the destination EID-s and the corresponding destination RLOC. This is done by using a (distributed) mapping 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 Home Agents in Mobile IP.

The mapping system uses a system similar to DNS: LISP Delegated Database Tree (LISP DDT), as visible in Figure 1.

The mobility is based on three phases/states of the mobile node [14].

(1) Registration and Getting a RLOC. Each mobile node in LISP has to be configured with at least an EID. This is a unique identifier, independent of the location. If the node has a classic DNS entry (in case this identifier is an IPv4 or IPv6 address) then the DNS system will return this IP address. The EID is assigned by the MS. In order to have Internet access the node also needs an RLOC, which is dependent on the location, so it will change in case of roaming. This can be obtained via traditional methods like DHCP. For each new RLOC obtained by the mobile node, the MS must be informed with a signalling message which includes the EID and the RLOC address. A node can have multiple RLOC's in case of multihoming. To avoid authentication problems, both the mobile node and the MS use a preshared key.

(2) For Each New RLOC Obtained, the LISP Node Has to Inform the MS about This New EID-RLOC Pair. A signalling message is defined which includes both the EID and RLOC address. It is possible for an EID to have multiple RLOC-s in case of multihoming. To ensure authentication, the LISP mobile node and the MS are configured with a preshared key. From the moment when the MS gets a valid registration request, the node is accessible in the network.

(3a) Signalling the EID-RLOC Pairs and the Data Transmission. Once an EID-RLOC pair is recorded in the MS, the LISP Mobile Node can start to send and receive data packets.

The sending node receives the address of the destination mobile node by querying the DNS server and then it sends the packet to this address. The packet is routed all the way to the xTR router (Tunnel Router) which verifies if it has the information about the destination EID's location. For this purpose each xTR saves in its cache memory the EID-RLOC pairs already used. If this information is not found in the cache memory, the xTR will send a Map-Request message to the MR (usually colocated with the MS). The MR will send then this message through the mapping system to the server which provides the information for the respective node. The MS builds a response message which includes the EID of the destination node, the RLOC addresses, the priority, and the weight of each RLOC link. This information is used for load sharing and load balancing. The response is sent directly to the xTR router, which will add this link to the cache memory and will use it to encapsulate the packets sent to the destination mobile node. For the received packets the same steps are followed to configure the route.

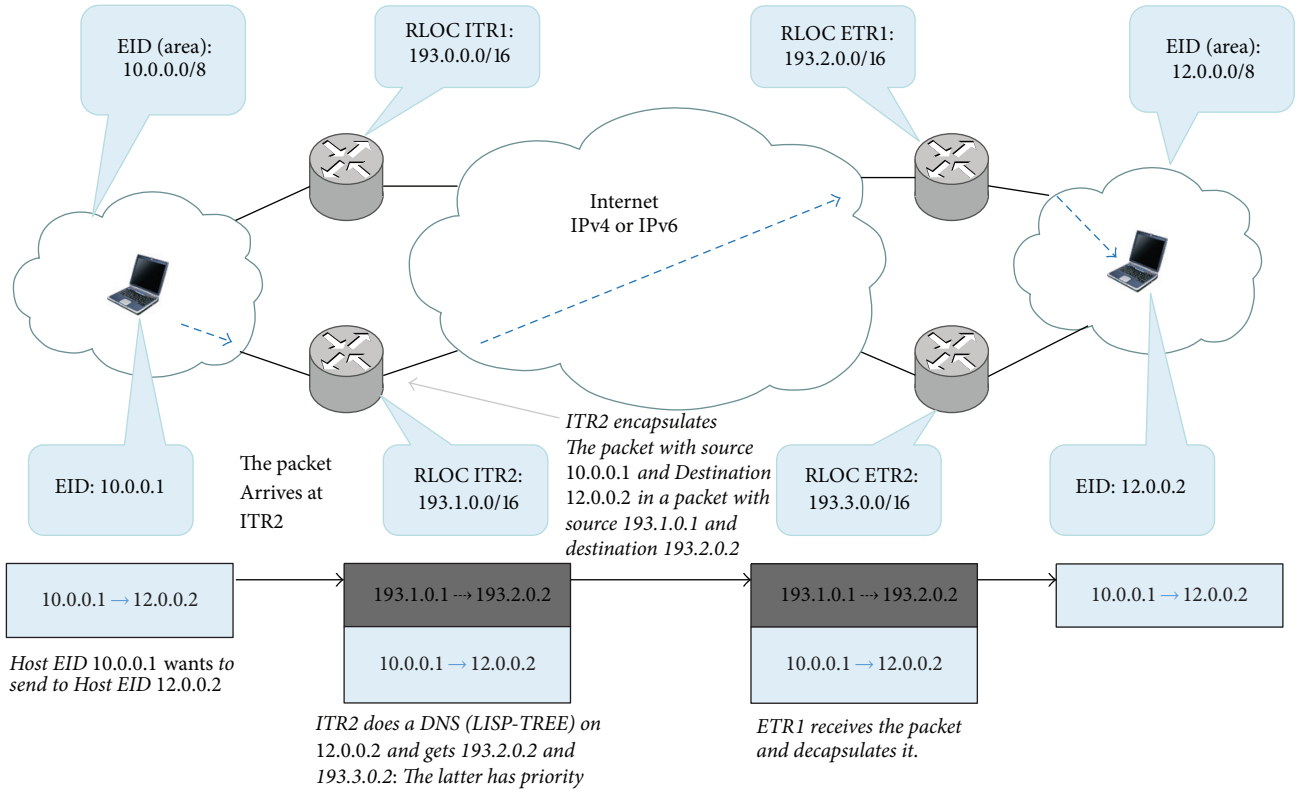

Figure 1: LISP data packet transmission.

(3b) Handover. If a mobile node changes the access point to the network, it will keep its connectivity even in a network served by another operator. If this is the case, a new RLOC will be assigned as mentioned earlier, paragraph (3a). This record will be sent to the MS. To update the routing information in all the routers that are used for communication, the node also sends the message SMR, Solicit Map Request. This will trigger an update of all EID-RLOC records in the cache memory of all routers involved, so that all the existing connections are kept.

As expressed in RFC 6830 ≪No changes are required to either host protocol stacks or to the "core" of the Internet infrastructure.

The Locator/ID Separation Protocol (LISP) can be incrementally deployed, without a "flag day"≫ [6]. So only some elements (routers) in the network need to know the LISP protocol, or only a mobile device, in case the LISP-MN option of the protocol is used.

Another important advantage of LISP is the support for QoS and Traffic Engineering for traffic in the core network (without the need of MPLS protocol usage).

3. Implementing a LISP Multihomed and Load-Balanced Demonstrator

In order to demonstrate the benefits of LISP compared to other routing protocols, but also to validate security and load-balancing solutions, we have implemented a simulated demonstrator based on Cisco devices supporting LISP.

The demonstrator is illustrative for the LISP configuration and functionality and can be applied for several scenarios, from distributed enterprise offices to the mobility use-cases described in the next sections.

Our objective was to test the LISP multihoming using two Internet service providers, but also to ensure encrypted communications, fail-over mechanisms, load-balancing and, not least, lower costs. Besides LISP functionality we can mention GET-VPN technology in order to provide network security and GLBP (Gateway Load Balancing Protocol) for load-balancing.

To be closer to a real-life scenario, we have described a network appropriate to an organization with several offices in different locations, as visible in Figure 2. This scenario answers the increasing need of many companies to outsource part of their processes and to build branches in countries where labor is much cheaper. The demonstrator architecture includes the headquarters and two branches, interconnected via the Internet [15].

As shown in Figure 2, the two branch sites are connected to the network using the routers Site 1 and Site 2, each of them having two different RLOC-s to ensure load balancing.

The Site 1 router acts as xTR for the two cloud networks, and the internal addresses (EID) inside the cloud networks are registered in the mapping system (Map Server) with the two RLOC-s. Load balancing is performed using a parameter that distributes 50% of the traffic per RLOC connection.

In order to encrypt intersites traffic via Internet, it was used a GET-VPN (Group Encrypted Transport VPN) [16].

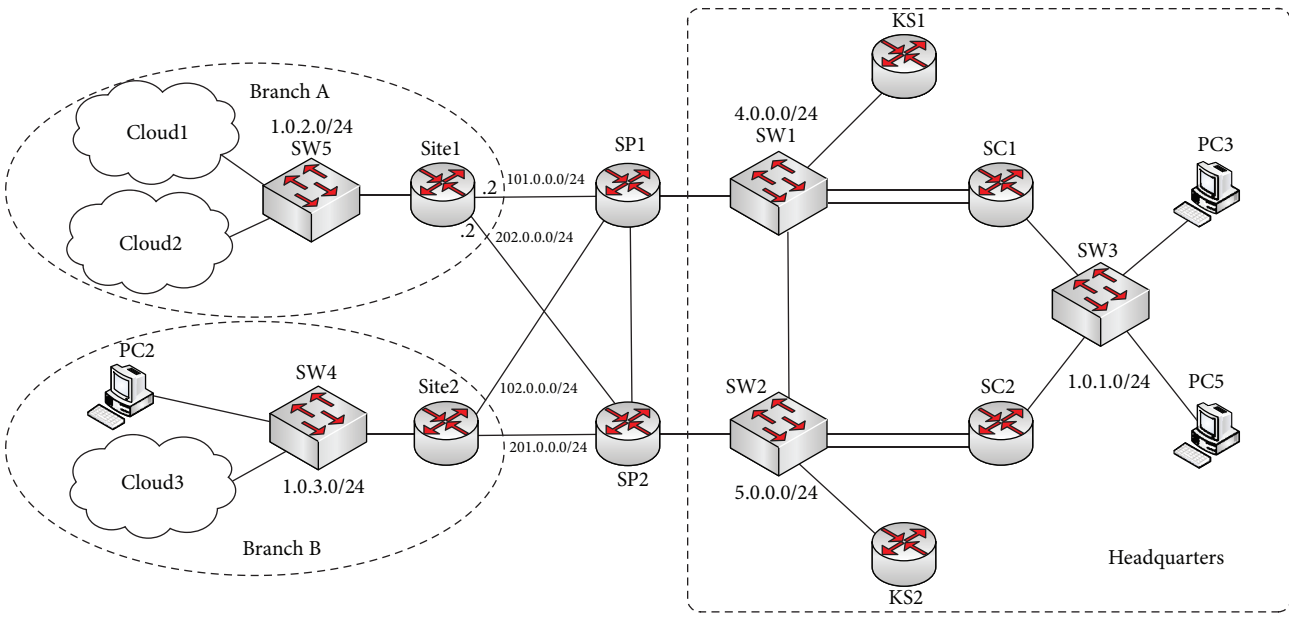

Figure 2: The multisite network demonstrator, running in GNS3 emulator.

To ensure fail-over and load-balancing over LAN (Local Area Networks) it was used GLBP (Gateway Load Balancing Protocol) [17] and an IP SLA (Internet Protocol Service Level Agreement). A big advantage of this implementation is that the BGP (Border Gateway Protocol) is no more needed to provide multihoming.

In order to simulate a realistic architecture we have chosen the GNS3 [18] graphic emulator, an open-source software that enables complex networks emulation. GNS3 emulates CISCO IOS systems that can be run on any computer, enabling network architects to test various configurations and protocols in a secure environment without the need of investing in laboratory hardware. The core of this program is Dynamips, an emulator of the IOS images.

The Cisco routers with IOS 15.x supporting LISP are, for instance, the types 1941, 29xx, and 7200 (and even some models of the 800 series). For the demonstrator architecture we have chosen 7200 series routers, as they not only support LISP (as real equipment) but are also fully supported by GNS3 (as emulated equipment).

In the demonstrator architecture shown above, simulated by GNS3, the two routers at the headquarters (SC1 and SC2) were configured to act as xTR-s (performing en/decapsulation of LISP packets from/to the headquarters hosts) and to provide load balancing.

On the other hand, remote (branch) locations are connected to the Internet via routers Site 1 and Site 2 that behave like xTR-s and have redundant connections to two Internet service providers SP1 and SP2. Mapping is provided by the SC1 and SC2 routers, each configured as Map Server and Map Resolver, that receive mapping requests from the RLOC routers and respond with a combination of the EID of the looked-for host and the address of the RLOC having behind it this EID.

Routers KS1 and KS2 play the roles of Map Server and Map Resolver, also managing the keys needed to encrypt the traffic in the GET-VPN.

3.1. The Headquarters. At the headquarters, the SC1 and SC2 routers act as RLOC for the PC3 and PC5 hosts; KS1 and KS2 are providing the keys and security policies for the operation of GET VPN.

In order to configure the SC1 router to act as an xTR, after all connections were accomplished, the following commands were sent to the console:

```
router lisp
loc-reach-algorithm rloc-probing
 database-mapping 1.0.1.0/24 4.0.0.2 priority 1 weight 50
 database-mapping 1.0.1.0/24 5.0.0.2 priority 1 weight 50
```

As can be noticed from the database-mapping commands above, hosts 1.0.1.0/24 from the headquarters network are mapped to two different RLOC: 4.0.0.2 and 5.0.0.2 which means that, in the Internet, packets for these hosts are sent to one of the two above-listed addresses. On the two connections there can be configured as well priorities

```
SC2#sh ip lisp map-cache
LISP IPv4 Mapping Cache for EID-table default (IID 0), 3 entries

0.0.0.0/0, uptime: 01:16:44, expires: never, via static send map-request
  Negative cache entry, action: send-map-request
1.0.3.0/24, uptime: 00:35:44, expires: 23:46:43, via map-reply, complete
  Locator    Uptime    State      Pri/Wgt
  102.0.0.2  00:35:44  up           1/50
  201.0.0.2  00:35:44  up           1/50
```

Figure 3: Records from the cache memory of the RLOC SC2 router.

and weights depending on the nature of existing traffic. For demonstration purpose, we have configured these two connections with equal priority and with 50% weights for traffic sharing on the two RLOC-s. However, one of the big advantages of LISP is the dynamic relocation of weights during the mobility process, more specific, the adaptation of the infrastructure (processes, data centers, and virtual machines) to the end-point mobility. This benefit would be highlighted in a dynamic configuration like the Public Transportation use-case that is detailed below, in paragraph 4, where the info exchange or data streaming servers are load-balanced based on end-user attachment in the network.

LISP stores in the cache memory of the RLOC router the identity mapping of the hosts. If a locator fails, this mapping is no longer usable and traffic would be lost. To solve this problem and to keep the consistency of mapping information, we used the command "loc-reach-algorithm rloc-probing". This command sends periodically messages of mapping request and replaces the locators that are no more functional in the table stored in the cache memory.

As mentioned in Figure 3, the SC1 and SC2 routers are configured to be part of the mapping system. Thus they are configured as Map Server and Map Resolver with the following commands:

```
ipv4 itr map-resolver 4.0.0.2
ipv4 itr map-resolver 5.0.0.2
ipv4 itr
ipv4 etr map-server 4.0.0.2 key demonstrator
ipv4 etr map-server 5.0.0.2 key demonstrator
ipv4 etr
exit
```

3.2. The Wide Area Network. The WAN consists of two routers SP1 and SP2 simulating the existence of two different service providers. Each router is connected through an interface with the headquarters. These two routers are configured to achieve simple routing between the two sites.

The Site 1 router is configured as a gateway for location 1 (branch 1) hosts and has two WAN connections, one for each Internet service provider (SP1 and SP2). LISP is configured on this router in order to behave like xTR and to map the network prefix EID 1.0.2.0/24 to the two available RLOC addresses: 101.0.0.2 and 202.0.0.2. Load balancing is performed using weighting parameters to distribute 50% of traffic per each RLOC connection.

The Site 1 router is also configured to be included in the security group V4GROUP; the recording interface is the Loopback one and server's addresses are 100.0.1.3 and 100.0.1.4 (see Figure 4).

```
router lisp
site headquarter
authentication-key demonstrator
eid-prefix 100.0.1.0/24
eid-prefix 1.0.1.0/24
exit
site site1
authentication-key demonstrator
eid-prefix 1.0.2.0/24
eid-prefix 1.1.1.1/32
exit
site site2
authentication-key demonstrator
eid-prefix 1.0.3.0/24
eid-prefix 2.2.2.2/32
exit
```

Since SC1 is in the same time RLOC for headquarters but also MS/MR we have added in the "router lisp" section the following commands:

Inside the two cloud networks there may be a variable number of hosts and creating, deleting, modifying, or migration of a host from Cloud 1 to Cloud 2 has no repercussions on the routing in the WAN or in the headquarters.

By using LISP the host identity is separated from the host location. Thus the host 1.0.2.3, defined on Cloud 1, can be migrated to Cloud 2, using the same IP address. In the mapping system, address 1.0.2.3 is assigned to the RLOC addresses 101.0.0.2 and 202.0.0.2 RLOC that remain unchanged during and after migration.

The separation between the control plane and data plane can be seen in the Wireshark capture (see Figures 5 and 6). If we analyse the ICMP ECHO message on interface that connects Site 2 RLOC to SP1 we notice that port lisp-date 4341 is used, while in a Map request message from the control plane we notice the use of control port 4342.

```
Site1>sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        101.0.0.2       YES NVRAM  up                    up
FastEthernet0/1        202.0.0.2       YES NVRAM  up                    up
FastEthernet1/0        1.0.2.1         YES NVRAM  up                    up
FastEthernet1/1        unassigned      YES unset  administratively down down
FastEthernet2/0        unassigned      YES unset  administratively down down
LISP0                  1.1.1.1         YES unset  up                    up
Loopback0              1.1.1.1         YES NVRAM  up                    up
```

Figure 4: The configuration of the Site 1 router interfaces.

```
User Datagram Protocol, Src Port: 13320 (13320), Dst Port: lisp-data (4341)
    Source port: 13320 (13320)
    Destination port: lisp-data (4341)
    Length: 220
  Checksum: 0x0000 (none)
Locator/ID Separation Protocol (Data)
```

Figure 5: Lisp data.

```
User Datagram Protocol, Src Port: lisp-control (4342), Dst Port: lisp-control (4342)
    Source port: lisp-control (4342)
    Destination port: lisp-control (4342)
    Length: 42
  Checksum: 0x7618 [validation disabled]
Locator/ID Separation Protocol
```

Figure 6: Lisp control.

```
Frame 4: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
Ethernet II, Src: ca:02:17:8c:00:1c (ca:02:17:8c:00:1c), Dst: ca:05:0f:68:00:00 (ca:05:0f:68:00:0
Internet Protocol Version 4, Src: 1.0.1.10 (1.0.1.10), Dst: 1.0.3.2 (1.0.3.2)
Internet Control Message Protocol
```

Figure 7: Structure of the packets sent between host and locator.

```
Frame 229: 254 bytes on wire (2032 bits), 254 bytes captured (2032 bits) on interface 0
Ethernet II, Src: ca:04:0a:3c:00:54 (ca:04:0a:3c:00:54), Dst: ca:03:0a:3c:00:54 (ca:03:0a:3c:00:
Internet Protocol Version 4, Src: 201.0.0.2 (201.0.0.2), Dst: 4.0.0.2 (4.0.0.2)
User Datagram Protocol, Src Port: 13320 (13320), Dst Port: lisp-data (4341)
Locator/ID Separation Protocol (Data)
Internet Protocol Version 4, Src: 1.0.3.2 (1.0.3.2), Dst: 1.0.1.10 (1.0.1.10)
Encapsulating Security Payload
```

Figure 8: GET VPN encrypted packets using EID and RLOC addresses.

On the interface between the host and the locator router the packets are sent with EID source and destination address and without GET VPN encryption. Such a packet has the structure shown in Figure 7 (before encryption and encapsulation).

LISP packets encapsulation and the use of EID and RLOC addresses can be observed on captured data packets (see Figure 8). Thus the existence of the information encrypted with GET VPN can be noticed. The ESP packet is encapsulated in an IP packet with an EID type source and destination, and then LISP is using port 4341 to encapsulate this packet into a new packet that is using this time RLOC addresses for the two EID-s.

```
glbp 1 ip 10.0.10.254
 glbp 1 timers 1 3
 glbp 1 preempt
 glbp 1 weighting 254 lower 10 upper 250
 glbp 1 load-balancing weighted
 glbp 1 weighting track 10 decrement 250
 glbp 1 forwarder preempt delay minimum 3
ip sla 10
```

3.3. Configuring Load Balancing with GLBP. For the LAN we have configured GLBP to provide load balancing and redundancy for the hosts. GLBP stands for Gateway Load Balancing Protocol and is a protocol for virtual gateways, similar to HSRP (Hot Standby Router Protocol) or VRRP (Virtual Router Redundancy Protocol).

However, compared with these protocols, GLBP is able to use more physical gateways simultaneously. The usage as VRRP in combination with LISP for redundancy was previously described [19], but we have considered GLBP implementation more appropriate. In HSRP and VRRP a group can have a virtual gateway with a single IP address and a single MAC address; only one physical gateway is responsible for routing packets, while the other gateways in the group remain in an inactive state as long as the used gateway works properly; thus, the bandwidth of these inactive routers is unused by the protocol. GLBP improves this process by allowing more virtual gateways to simultaneously take part in packets routing and perform load balancing across multiple routers (ports) using a single virtual IP address and more virtual MAC addresses [20]. Each host is configured with the same virtual IP address, and all routers in the group participate in routing packets. GLBP members communicate with each other through "hello messages" sent every 3 seconds to the multicast address 224.0.0.102, port 3222.

The members of a GLBP group choose one gateway to be the AVG (Active Virtual Gateway). The other group members become redundant for the active gateway and become active if the AVG fails. AVG assigns a virtual MAC address to each member of the GLBP group and each of these members, known as AVF (Active Virtual Forwarders). GLBP provides redundancy to the virtual gateways, similar to HSRP. GLBP uses a weighting scheme to determine the forwarding capacity of each router in the group. Inside a GLBP group, weights can be adjusted automatically by monitoring the state of a router's interface. If the monitored interface is no longer functional, the weight is reduced by a specified amount. There can be monitored more interfaces so that the weights can be adjusted with different values.

In order to activate GLBP the command "ip glbp" was sent to the interface FA1/0 towards the hosts of the headquarters. The selected virtual address was 1.0.1.254. It was then set the interval between "hello messages" at 1 second to get a quicker response, these messages being valid for 3 seconds ("holdtime"); the preconfigured values are 3 and 10 seconds, respectively. Through these "hello messages" the routers are learning the virtual address.

```
 icmp-echo 1.0.0.1
 threshold 800
 timeout 1000
 frequency 2
ip sla schedule 10 life forever start-time now
track 10 ip sla 10
```

We have enabled "preemption" in the process of choosing an AVG that is disabled by default. This can allow a higher priority router to become the active gateway even if the current one is still functional. We activated the method of load balancing on the two paths using the "glbp one load-balancing" command. There are three options: host-dependent, round robin, and weighted. We have chosen the latter, to make the hosts accessible even if one of the routers has a problem. To track the availability of the WAN connection, IP SLA is used with ICMP probes. In case the IP SLA probe fails, the active forwarder is passed to the other router.

3.4. Providing Network Security Using GET VPN. Network security is essential especially for applications in the area of public safety. Most of the encryption techniques are based on tunneling, at Level 2 or at Level 3. But as we were dealing with Cisco routers, we considered that the most suitable solution for network security is by the usage of Cisco GET-VPN technology that is a tunnel-less VPN technology, providing end-to-end security for network traffic in a native mode and maintaining the fully meshed topology, as visible in Figure 3.

Communications security is ensured by using GET VPN together with GDOI (Group Domain Of Identification). The Cisco GET VPN [21] introduces the concept of trusted group in order to avoid point-to-point tunnels and overlay routing associated with the existence of these tunnels.

All group members (GM-s) share a common security association (SA). This allows GM-s to decrypt traffic encrypted by another GM.

The benefits of GET VPN are important especially for multicast infrastructures. GET VPN is an instant large-scale mesh connectivity paradigm using the group IPsec paradigm (see Figure 9).

GDOI protocol is used for Group key and group SA management. GDOI is based on ISAKMP (Internet Security Association Key Management Protocol) for the authentication of the KSs and GMs. All the standard ISAKMP authentication schemes like RSA Signature (certificates) and preshared key can be used for GETVPN.

This way GET VPN is very well integrated with QoS and traffic engineering capabilities. GDOI key management protocol is used to providing a set of encryption keys and policies for a group of devices.

GET-VPN needs an interface to source traffic destined for the KS. Because Site 1 and Site 2 routers have dual WAN connections, but only one interface can be specified for GET VPN, we chose to use loopback interfaces for registration. Because routers Site 1 and Site 2 have no direct connection to the headquarters (where KS1 and KS2 are implemented), having only Internet connections, it is possible to create GRE tunnels from the KS-s in the headquarters to the branch sites. However, this option is not the most favourable, so we have chosen to add the loopback interfaces of the two sites routers in the configuration of the MS-s, these being treated like sites prefixes.

In the headquarters, we have also integrated the two KS-s that are configured to define security policies and to generate keys for GDOI GM-s. Each RLOC (SC1, SC2, Site 1, and Site 2) is part of this group and is authenticated to one of the KS-s receiving a key (unique for all GM-s) that encrypts the network traffic.

In order to configure network security we have first defined an Internet Key Exchange (IKE) policy number 10, for authentication with preknown AES (Advanced Encryption Standard) 256-bit keys, the group number being 1.

The key system is the most important element of GET VPN as it plays a central role in the control plane. Thus, a single KS should be "single point of failure" for a network based on GET VPN. Being obvious that KS-s redundancy is very important, GET VPN offers support for COOP KS (multiple cooperative KS-s). For this purpose a redundant server (KS2) was provided.

```
redundancy
    local priority 100
     peer address ipv4 100.0.1.4
```

Communication between the two KS-s is ensured by the interface that connects the two switches (SW1 and SW2). If configuring is done correctly, starting KS1 is followed by a GDOI activation message, starting message for the process of choosing a primary KS, and acknowledgement of primary KS for the GDOI group.

4. Smart Mobility Use-Case: Internet for Public Transportation

Internet for public transportation [22], sometimes perceived as "free WiFi" by users of mobile transportation vehicles, is not something new, but the evolution of services is triggering a response also in the network architecture [23].

More and more sophisticated applications are launched and used, while social networking, popular online video services and video/content on demand (e.g., Netflix) are very highly ranked in the preferences of modern users. All these are bandwidth-intensive activities that, combined with high number of mobile-handover procedures, typical for

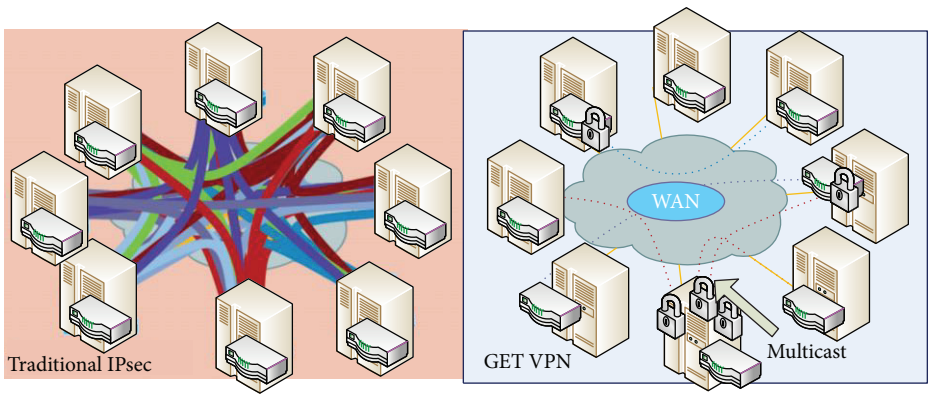

Figure 9: Traditional IP-Sec versus the tunnel-less GET VPN technology.

public transportation vehicles, are a challenge for the Internet Service Providers.

Popularity of mobile streaming and increase of on-board infotainment (that could include relevant trip information to passengers) has also changed the service ecosystem around transportation, including now the rail service partner (including maybe a multimedia content provider), the rail infrastructure provider and the train manufacturer/train monitoring, and maintenance partner.

But besides the commercial and end-user aspects, there are important IP broadband requirements from Mission Critical Communications applications [24]. The mobile connection is considered the basic layer ("data pipe") for a series of applications including infrastructure management, security and surveillance, signaling, and secure communications.

Today LTE (Long-Term Evolution) communications became the dominant standard for broadband data transfer, streaming, in public mobile radio business and is already accepted as the standard for the future evolution of TETRA (Terrestrial Trunked Radio). The radio system for railways, GSM-R (Global System for Mobile, Railways), and constituent parts of ERTMS (European Rail Traffic Management System) are considered also evolution to LTE or even to future 5G technologies [25].

Additional services could be related to machine-to-machine (M2M) communications. Possible applications include monitoring vehicle (and environment) parameters, and fleet management, with contained GPS receivers.

Public safety organizations especially but also utility and transport companies are asking for multimedia data, streaming, applications in order to optimize their daily operations (mobile data applications could increase productivity, while in a public safety scenario broadband helps to increase the situational awareness of an officer in the field or at the command center). Examples of applications that include video streaming ("CCTV on scene") are "ad-hoc real-time relaying of surveillance camera stream to patrol cars" or "upstream video from patrol cars to the command and control center." Other examples of applications could include online access to building plans and other relevant information during emergency operations, remote passport and finger print checks, sending biometric data, and so forth.

So the security and reliability of broadband solutions for public transportation become very important characteristics for the public safety and critical communications area, while the demand for these services is increased with the recent global terrorism threads.

Train operators have started to request higher SLA and QoS for the services [26], especially because some of them include the pay-per-view charging systems [27]. So, the reliability of Internet connection is an important attribute of the solution. Besides the different caching solutions (local multimedia content, usage of WAN accelerators), the solution could not rely solely on the usage of one Internet service provider; thus load-balanced multihomed connections (and not only back-up routes) are needed.

Here LISP mobility [28] brings its advantages, while it offers solutions for maintaining the IP addresses of users while roaming and also offers the possibility to use simultaneously and load-balanced, two Internet service providers to connect to the multimedia streaming location or to a specific datacenter.

4.1. Typical Vehicle-to-Ground Communication Architecture. In Figure 10, we tried to synthetize the typical requirements and architecture for a train/bus communication architecture and in the next paragraph we will present the envisioned optimized architecture based on the LISP protocol. The scenario considers a train wagon or bus, having two WAN routers, connected via a secure connection to a Backend network and further to a multimedia streaming content server or application server and to the Internet.

Because of the many challenges to connectivity whilst on a train (signal blocking due to the metal body of the train, a lot of people on the same train are competing for the connectivity, mobility, and different travel conditions like tunnels) the solution for passengers is to connect to on-board WiFi that is further connected to internet via mobile WAN routers. This brings also other advantages like the easiness to register for users and subsequently automatically join the possibility of a captive portal usage for authentication and charging/payment topics.

WAN routers can be physically placed with distance between them (for train connectivity, the recommended case

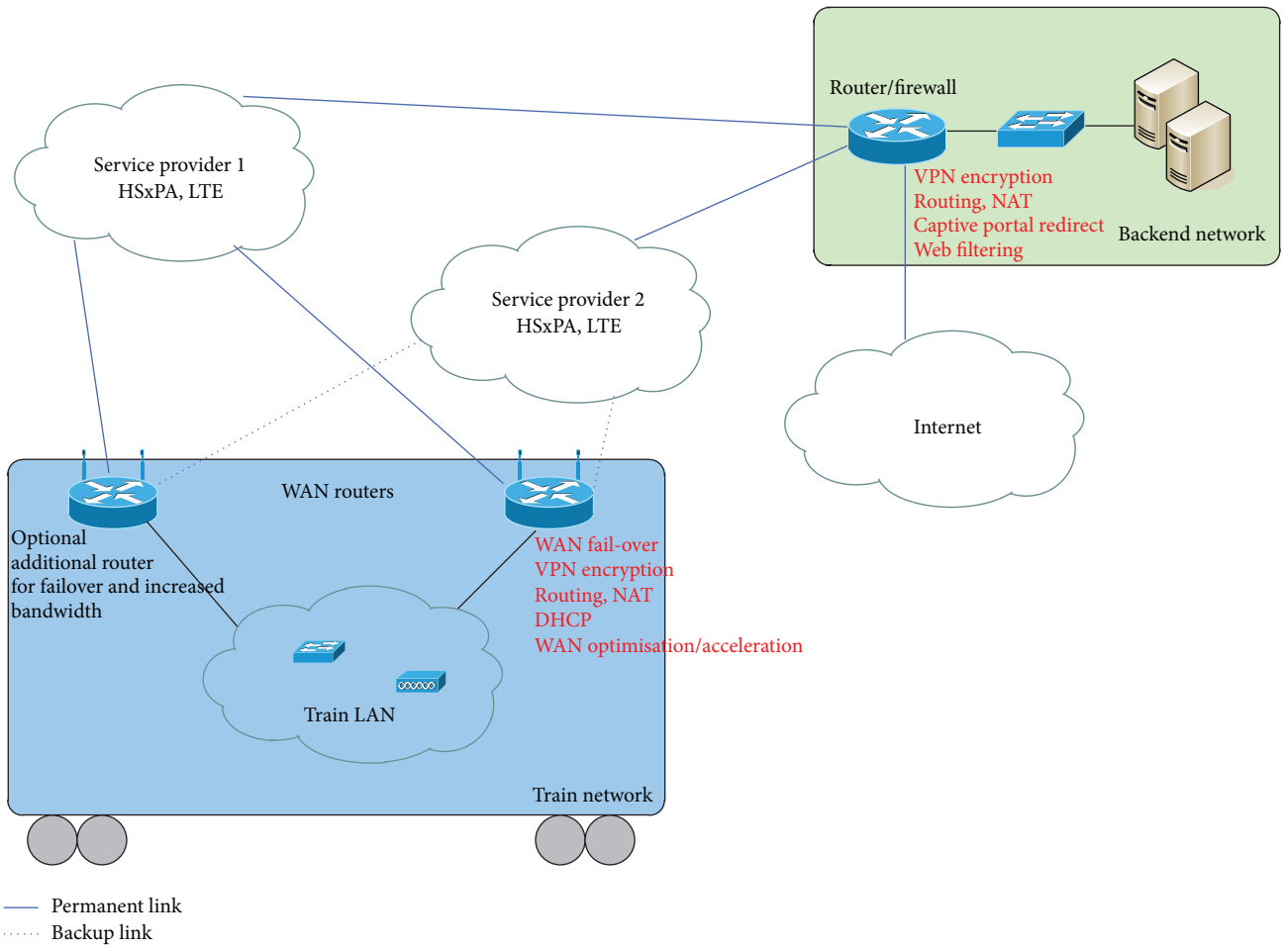

Figure 10: Typical Vehicle-to-Ground Communication Architecture.

is using 2 or more routers). For the train case, communication between wagons is possible though the wireless or wired couplings between the wagons. WAN routers (as all train equipment) are rugged and a common requirement is to comply with the EN50155 railway standard (this is why not all vendors qualify and there are dedicated/industrial rugged in-train equipment manufacturers, e.g., MOXA [29]). The WAN routers provide communication with the back-end network but also services like IP assignment or DNS caching to LAN clients.

In the typical scenario, the WAN router has 2 SIM cards from different service providers, one active and the second one going online after the primary connection fails (SLA connection monitoring). Connection selection and type configuration is very flexible. So in the typical scenario just per-connection failover is offered, as a back-up, but not a real load-balancing of multihomed connections. Switching times between connections are in the range of seconds; nevertheless, in the case mobile signal strength is very low on the primary interface but connection is not completely lost, the switching to the other interface will not take place. Via scripting, primary connection can be chosen based on coverage type: LTE, HSxPA, and so forth, but real load-balancing is not performed. This is possible by using the LISP protocol for multihoming as it will be described in the next paragraph. Both encrypted and unencrypted connections are available/necessary, but for public safety scenarios the traffic should be encrypted.

Another important element used for mobile connections in public transportation vehicles are the WAN Optimization techniques (also known as WAN accelerators), which could bring real benefit for saving the traffic bandwidth. The techniques used by WAN Optimization include de-duplication (in order to eliminate the transfer of redundant data across the WAN), compression, latency optimization (e.g., TCP refinements such as window-size scaling, selective acknowledgements, Layer 3 congestion control algorithms), proxy/cache, forward error correction (mitigates packet loss, reduces retransmission), application traffic shaping, and equalizing (assumes what needs immediate priority based on data usage).

Back-end network provides Internet connectivity with address translation and web filtering (filter out bandwidth-intensive media sites, banned content). This is the reason to

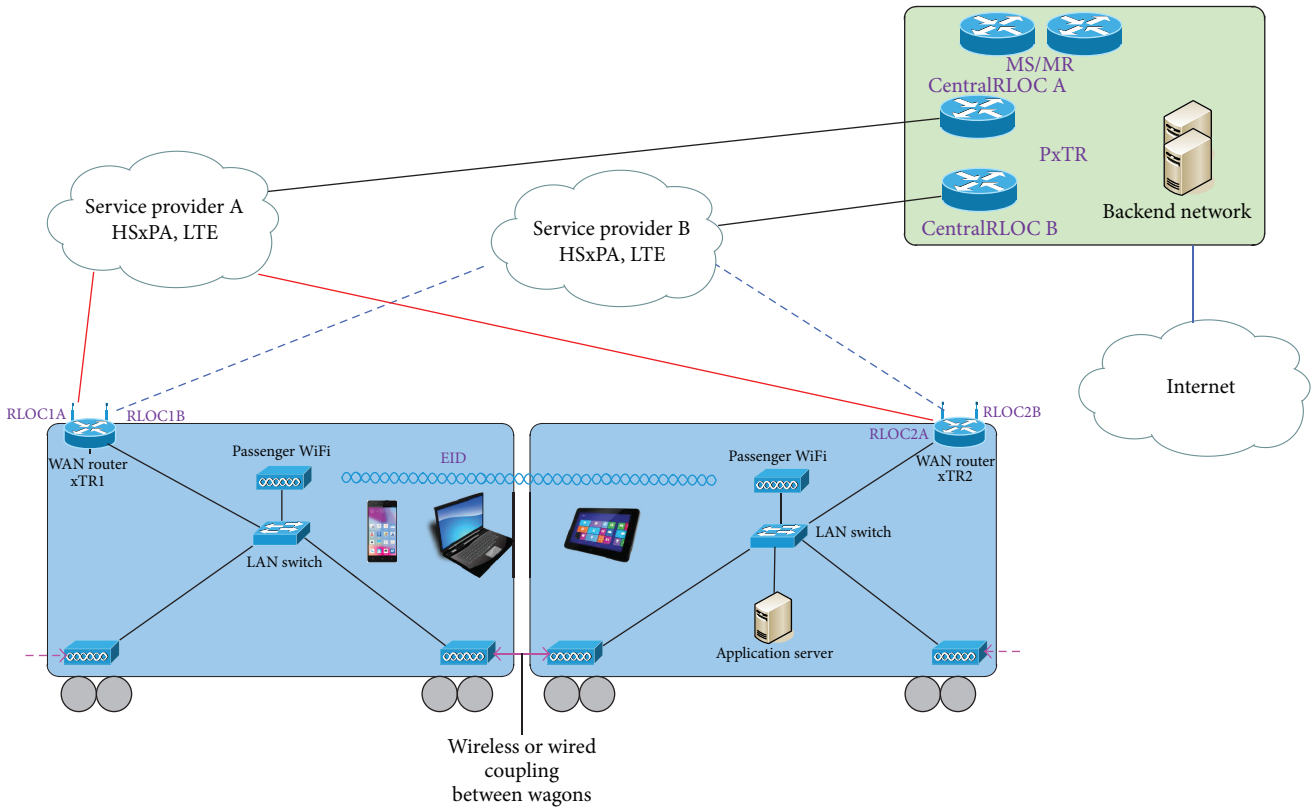

Figure 11: LISP-based architecture deployed inside public transportation system.

bypass the Internet traffic via the back-end element. Also as part of back-end element we should mention the application servers (e.g., multimedia streaming content server; video recording server) but also there are included functions like network management and monitoring (alarming, bandwidth monitoring, logging, on-board device monitoring) and statistics, data analytics, or even DPI (deep packet inspection) servers. The back-end network is able to connect to train routers with dual service providers in order to provide load balancing and failover.

While the infotainment service usage (passenger information and entertainment) is considered to be higher in trains, for the bus scenario the travel route is not always fixed (like the train rails), so the mobile network coverage may differ; thus real-time load-balancing between Internet service providers using LISP multihoming could bring more advantages.

4.2. LISP Architecture for Public Transportation Network Mobility. In this section we propose an adapted in-train architecture detailing the LISP elements implementation for the mobility use case. The IP addresses role designation is done as follows: each WAN router plays the role of an xTR and has 2 mobile interfaces; this is why a 2SIM router would be a good solution (example of a commercial solution would be the Cisco C819 model that has also LISP support). Each of these interfaces has defined RLOC addresses, while the "in-train" network, based on WiFi with possible switched distribution network for coupling between wagons, would be using EID addresses in a certain address range. The back-end network represents not only a proxy to Internet, but also acts as firewall and accommodates the application servers. From LISP perspective the back-end network represents the RLOCs to the central location, similar with SC1 and SC2 in the headquarters for the GNS3 demonstrator that was presented above. The back-end should include also the MS/MR standalone (as represented in Figure 11) or colocated with other elements.

LISP allows transparently integration of IPv4 and IPv6 addresses, so both types of addresses can be used. With regard to secure connectivity, most likely mobile data VPN should be used (layer 2 or layer 3 private network between mobile APN and backend network). However, the Cisco GET-VPN solution that we have implemented in our demonstrator presented in the previous section could bring great advantages, as it does not require an adjacent routing infrastructure for the control plane and integrates perfectly with multicast infrastructures that might be used in case of emergency for public security type of applications.

4.3. Proposal for Open LISP Implementation of Multihomed Load-Balanced Vehicular Internet. In our demonstrator we were able to validate the LISP solution for load-balanced multihomed enterprise environment, using two service providers for interconnection. We now extrapolate this use-case to a mobility scenario, involving the existing open implementations of LISP and LISP-MN. The mobility scenario is very similar with the distributed enterprise environment.

While our GNS3 testing was performed with Cisco devices, as LISP is an open protocol, 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 [30, 31] as one of them, but we have focused our attention to Open Overlay Router (OOR) [32], 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 [33]. OOR implements LISP data plane and LISP control functionality, but also offers support for LISP-MN for mobile node mobility; this is why it is very suitable for mobility cases, like the public transportation scenarios. Also OOR is not only a LISP implementation; it represents an ecosystem for overlay networks, integrated with Software Defined Networks [34] (OOR aims to be a key tool in SDN/NFV, Network Functions Virtualization [35] environments), more specific to OpenDaylight SDN Controller [36], one of the most developed open solutions of this type. Also it includes support for NETCONF/YANG protocol for network configuration and provisioning.

LISP-MN [37] leverages the mapping infrastructure of LISP to support mobile devices by turning the mobile device into a LISP ITR and ETR for itself. The mobile device sends map requests; all packets originating at the mobile device are LISP encapsulated and the mobile device can answer directly incoming Map requests, or it can designate its Map Server as a proxy.

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 identified two different scenarios, suitable to be implemented: usage of LISP-MN directly on the Android phone or enabling LISP on the WAN router that acts as xTR. The Android case, though very versatile and spectacular because all the jobs are performed by the smartphone, needs the preconfiguration of Android Open Overlay Router software on the device, so it is not optimal for passengers that are using the network on ad-hoc basis [38]. Also, as detailed in the previous paragraph, the typical scenario for passengers is to use the WiFi connection [39].

So the scenario that we propose is the usage of the OpenWRT implementation of OOR that runs on a mobile WAN router that includes also 3G/LTE mobile connection. We have chosen the TP-LINK models TL-MR3420 or TL-MR3020 (both supporting OpenWRT firmware), having the possibility to include a SIM card or an external USB 3G modem and offering also the advantage of portability and easiness to be included in real testing configurations due to miniaturization. However, because we have two RLOC-s at the WAN router level and we should use two service providers, there is a need for two WAN interfaces for the router.

This is why the solution chosen is to transform one Ethernet interface (cabled with a RJ45 plug) into a second WAN interface, thus permitting multihoming and load-balancing. In order to enable this, the solution would be the usage of the mwan3 package [40] or multiwan [41] in OpenWRT. The simplest way to do this is using to put individual switch ports into own VLANs, each of them becoming thus separate interfaces. Further, the cabled interface is then connected to a second WAN router with 3G/LTE connectivity via a second Internet service provider.

```
root@OpenWrt:~# mwan3 interfaces
Interface status:
Interface wan is online (tracking active)
Interface wan2 is online (tracking active)
```

Figure 12 depicts our proposed architecture for an open implementation. Central in our WAN network there is the SDN controller. All the benefits of Software Defined Networks are available via the dedicated OpenDayLight controller with support for LISP as part of the LISPFlowMappings module [42]. This approach opens up new perspectives, and traffic can be steered on-the-fly through different OORs by only interfacing with OpenDayLight. Incorporating the WAN Optimization techniques for accelerated delivery of all applications across the Software-Defined WAN over the core network of the LISP network is initially the most important. Software-defined WAN (SD-WAN) is a concept that combines the benefits of WAN optimization techniques (detailed above in Section 4.1) with the software-defined networking by virtualizing the WAN. Thus policies for WAN optimization can be described and dynamically adjusted at SDN controller level (e.g., OpenDaylight) and also functionality like WAN path control, transport-agnostic connectivity, management, and automation is enabled (e.g., aggregation of multiple Internet connections so that they function as a single virtual overlay with increased performance and reliability).

There are already existing commercial solutions and specific applications of software-defined networking (SDN) [43] technology applied to WAN connections (mainly at Cloud level) [36], and we can mention the Riverbed Steelconnect SD-WAN [44, 45], as Riverbed is one of the most well-known solution for WAN Optimisation.

OOR can also be used as xTR in the back-end location, but also as a basic MS/MR where configured EID prefixes can be registered by xTRs. OOR will also reply to MapRequests addressed to those prefixes.

Example of typical LISP interface configured for RLOC and for EID broadcast on Open Overlay Router:

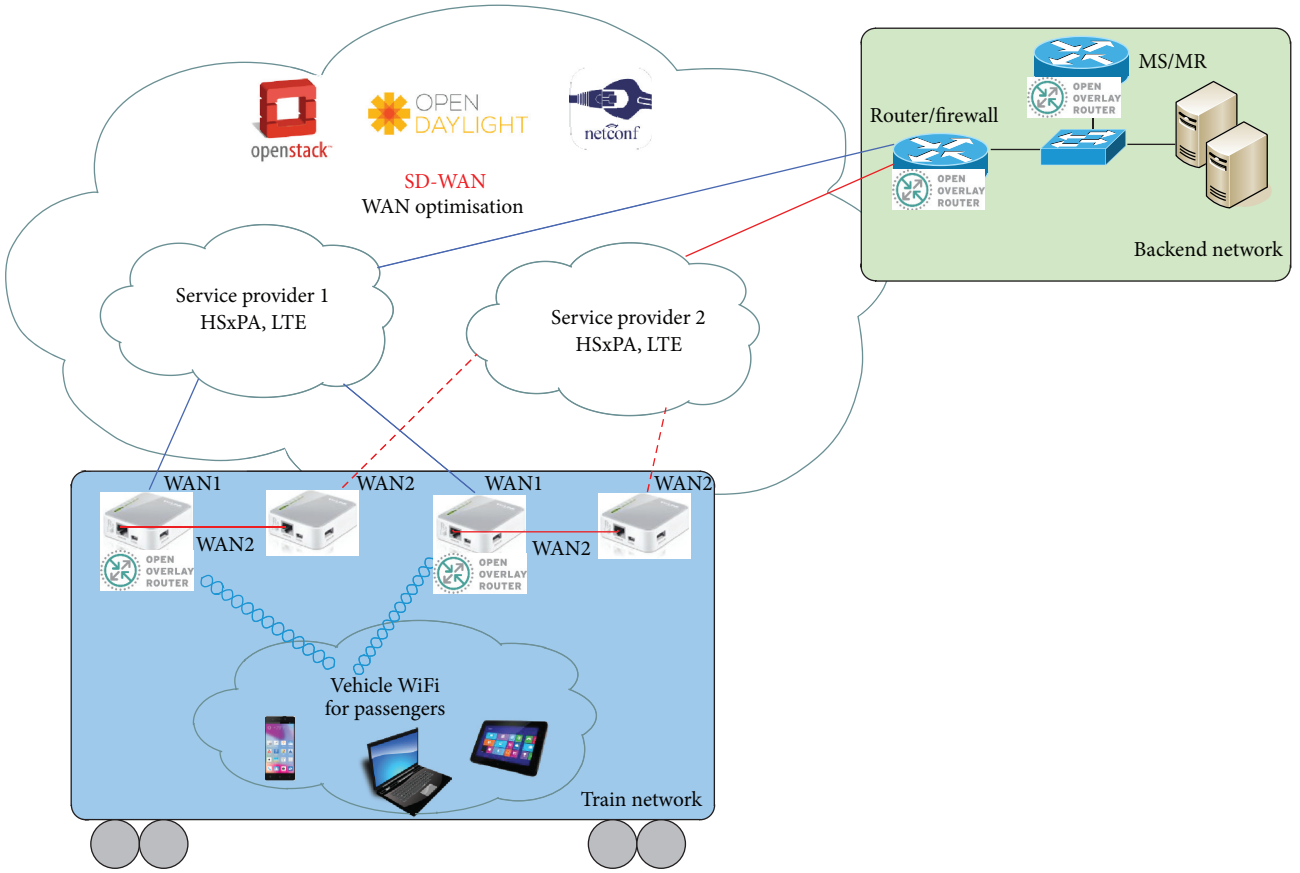

FIGURE 12: Simple prototyping of in-vehicle LISP configuration, based on open solutions.

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
    inet <RLOC> brd <RLOC_BROADCAST> scope global eth0
       valid_lft forever preferred_lft forever
eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 00:00:00:00:00:00 brd ff:ff:ff:ff:ff:ff
    inet <EID1> brd <EID1_BROADCAST> scope global eth0
       valid_lft forever preferred_lft forever
```

5. Conclusions and Further Development

The quality and reliability of connectivity for Public Transportation Systems becomes of major importance when correlated with commercial requirements and different service-level agreements (SLA), but mainly when the broadband connectivity is used for public safety and critical communication applications.

This paper makes a proposal for a network mobility architecture based on the LISP protocol aiming to find a solution that answers the following requirements: multihoming using multiple service providers, load balancing and encrypted connections. These were validated in a GNS3 demonstrator with Cisco7200 IOS with integrated LISP support. The traffic encryption was realized using Cisco GET VPN while the load balancing was realized using GLBP protocol. The architecture included one headquarters and two distributed enterprise locations, and further we have proven that these network connections with multi-homing could be also used for vehicle-to-ground communication in public transportation systems. The 2 distributed locations, both attached to two mobile service providers, could actually be two WAN routers installed in the vehicle (e.g., urban bus or sub-urban train). We have emphasized that the multihoming capability of LISP could have specific advantages beyond the simple handover to backup providers (neither the switchover

times nor the "hysteresis" in signal margins can be really "zero").

We have analysed the implications and specific requirements of resource-demanding services offered for public transportation scenarios, which can be extended to the area of mobile applications for public safety and the methods to implement LISP host mobility in a multihomed environment. Compared to other mobility solutions, we can notice the easiness of LISP implementation in existing networks, based on the simple mappings provided by the MR/MS mechanism, similar to the consolidated VLR/HLR (Visitor-/Home-Location Register) model in mobile communications, used to update temporary location registration.

We have proposed an open LISP implementation for the public transportation scenario based on Open Overlay Router, a solution that brings in all the advantages of software defined network by integration with an SDN controller. Most important aspect of our proposal is the existing implementation of OOR for mobile devices (Android smartphones); thus the LISP-MN version can be implemented directly at the edge of the network, with minimal impact for the network infrastructure.

Our further actions include validation of the open-source based architecture, but also testing more complex experimental configurations (including more xTRs) using Ixia IxNetwork [46] tool that has LISP MS/MR and xTR emulation support. For a through experimental validation we intend to test the proposed configurations in a real scenario, in a bus or in a train (with the support of our industrial partner, acknowledged below). It would be very interesting to monitor the traffic load balancing between the two mobile provider connections, in comparison with the parameters of the cellular network (that could be monitored based on signal strength).

One important enhancement for our work would be the usage of other type 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, an important unexploited advantage of LISP mappings.

Competing Interests

The authors declare that there is no conflict of interests 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.

References

[1] O. Vermesan and P. Friess, Eds., *Internet of Things: Converging Technologies for Smart Environments and Integrated Ecosystems*, River, Aalborg, Denmark, 2013.

[2] C. Mavromoustakis, G. Mastorakis, and J. M. Batalla, Eds., *Internet of Things (IoT) in 5G Mobile Technologies*, Springer, Cham, Switzerland, 2016.

[3] M. Gohar, J.-G. Choi, and S.-J. Koh, "An ID/locator separation based group mobility management in wireless body area network," *Journal of Sensors*, vol. 2015, Article ID 537205, 12 pages, 2015.

[4] S. Secci, K. Liu, and B. Jabbari, "Efficient inter-domain traffic engineering with transit-edge hierarchical routing," *Computer Networks*, vol. 57, no. 4, pp. 976–989, 2013.

[5] 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.

[6] T. Kondo, R. Aibara, K. Suga, and K. Maeda, "A mobility management system for the global live migration of virtual machine across multiple sites," in *Proceedings of the 38th Annual IEEE Computer Software and Applications Conference Workshops (COMPSACW '14)*, INSPEC 14600475, pp. 73–77, Vasteras, Sweden, July 2014.

[7] S. Murugesan and I. Bojanova, *Mobile Cloud Computing*, Wiley-IEEE Press, 2016.

[8] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "Locator/ID Separation Protocol (LISP)," draft-farinacci-lisp-12, Internet Engineering Task Force, RFC 6830, 2012.

[9] J. Rodriguez, Ed., *Fundamentals of 5G Mobile Networks*, John Wiley & Sons, 2015.

[10] A. Sniady and J. Soler, "An overview of GSM-R technology and its shortcomings," in *Proceedings of the 2012 12th International Conference on ITS Telecommunications (ITST '12)*, pp. 626–629, Taipei, Taiwan, November 2012.

[11] B. Quoitin, L. Iannone, C. De Launois, and O. Bonaventure, "Evaluating the benefits of the locator/identifier separation," in *Proceedings of the ACM SIGCOMM 2007 Workshops-2nd ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch '07)*, Whitepaper, Kyoto, Japan, August 2007.

[12] 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, no. 1, pp. 13–33, 2014.

[13] Cisco Whitepaper—LISP Overview, http://lisp.cisco.com/lisp_over.html.

[14] V. Jain, *A study of locator ID separation protocol [M.S. thesis]*, Kansas-City University, 2010.

[15] 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.

[16] http://www.cisco.com/en/US/docs/ios-xml/ios/sec_conn_getvpn/configuration/15-2mt/sec-get-vpn.html.

[17] P. Dubey, S. Sharma, and A. Sachdev, "Review of first hop redundancy protocol and their functionalities," *International Journal of Engineering Trends and Technology*, vol. 4, no. 5, 2013.

[18] GNS3 Emulator, https://www.gns3.com/.

[19] V. Veselý and O. Ryšavý, "Locator/Id split protocol improvement for high-availability environment," in *Proceedings of The 11th International Conference on Networking and Services (ICNS '15)*, pp. 61–67, The International Academy, Research and Industry Association, Roma, Italy, 2015.

[20] P. Lapukhov, GPLB Explained, http://blog.ine.com/2008/04/24/glbp-explained/.

[21] J. Nadhem, AlFardan (Cisco Systems), Advanced IPSec with GET VPN, http://www.menog.org/presentations/menog-2/nadhem-alfardan-get-vpn.pdf.

[22] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of vehicles: from intelligent grid to autonomous cars and vehicular clouds," in *Proceedings of the IEEE World Forum on Internet of Things (WF-IoT '14)*, pp. 241–246, Seoul, South Korea, March 2014.

[23] M. Fadda, M. Murroni, 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.

[24] M. Peltola and H. Hammainen, "Economic feasibility of mobile broadband network for public safety and security," in *Proceedings of the IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '15)*, INSPEC 15661194, pp. 67–74, Abu Dhabi, UAE, October 2015.

[25] A. Sniady and J. Soler, "Capacity gain with an alternative LTE railway communication network," in *Proceedings of the 7th International Workshop on Communication Technologies for Vehicles (Nets4Cars-Fall '14)*, INSPEC 14841718, pp. 54–58, St. Petersburg, Russia, October 2014.

[26] F. J. R. Tocado, A. D. Zayas, and P. M. Gomez, "Performance study of internet traffic on high speed railways," in *Proceedings of the 2013 IEEE 14th International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '13)*, pp. 1–9, Madrid, Spain, June 2013.

[27] M. Fadda, V. Popescu, M. Murroni, P. Angueira, and J. Morgade, "On the feasibility of unlicensed communications in the TV white space: field measurements in the UHF band," *International Journal of Digital Multimedia Broadcasting*, vol. 2015, Article ID 319387, 8 pages, 2015.

[28] D. Meyer, D. Lewis, and D. Farinacci, "LISP Mobile Node," draft-meyer-lisp-mn-06.txt, Internet Engineering Task Force, October 2011.

[29] http://www.moxa.com/.

[30] http://www.openlisp.org/.

[31] D. C. Phung, S. Secci, D. Saucez, and L. Iannone, "The OpenLISP control plane architecture," *IEEE Network*, vol. 28, no. 2, pp. 34–40, 2014.

[32] http://www.openoverlayrouter.org/.

[33] https://www.openwrt.org/.

[34] D. Thomas and K. G. Nadeau, *SDN: Software Defined Networks, an Authoritative Review of Network Programmability Technologies*, O'Reilly Media, August 2013.

[35] A. Falchetti, C. Azurdia-Meza, and S. Cespedes, "Vehicular cloud computing in the dawn of 5G," in *Proceedings of the IEEE Chilean Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON '15)*, pp. 301–305, Santiago, Chile, October 2015.

[36] https://www.opendaylight.org/.

[37] 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.

[38] S. Khalid, A. Mahboob, C. F. Azim, and A. Ur Rehman, "IDHOCNET: a novel ID centric architecture for ad hoc networks," *Journal of Computer Networks and Communications*, vol. 2016, Article ID 6438584, 18 pages, 2016.

[39] K. Li, S. Wang, and X. Wang, "Edge router selection and traffic engineering in LISP-capable networks," *Journal of Communications and Networks*, vol. 13, no. 6, pp. 612–620, 2011.

[40] https://wiki.openwrt.org/doc/howto/mwan3.

[41] https://wiki.openwrt.org/doc/uci/multiwan.

[42] https://wiki.opendaylight.org/view/OpenDaylight_Lisp_Flow_Mapping:Architecture.

[43] 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.

[44] Riverbed Steelconnect SD-WAN, http://www.riverbed.com/gb/products/steelconnect.html.

[45] http://www.riverbed.com/gb/press-releases/Riverbed-revolutionizes-networking-with-launch-of-new-application-defined-SD-WAN-solution-for-a-cloud-centric-world.html.

[46] IXIA IXNetwork DataSheet, https://www.ixiacom.com/sites/default/files/resources/datasheet/ixnetwork_overview_1.pdf.