FIRMS: A Mapping System for Future Internet Routing

Michael Menth, Matthias Hartmann, and Michael Höfling

***Abstract*—The locator/identifier split is a design principle for new routing architectures that make Internet routing more scalable. To find the location of a host, it requires a mapping system that returns appropriate locators in response to map-requests for specific identifiers. In this paper, we propose FIRMS, a "Future Internet Routing Mapping System". It is fast, scalable, reliable, secure, and it is able to relay initial packets. We introduce its design, show how it deals with partial failures, explain its security concept, and evaluate its scalability.**

***Index Terms*—Routing, Reliability, Locator/identifier split**

I. Introduction

ORGANIZATIONS usually receive IP addresses from the IP number space of their Internet service providers (ISPs). If they change ISPs, they get addresses from a different IP number space of their new ISPs. Thus, cumbersome renumbering of customer equipment is required. Otherwise, if users keep their IP addresses after the change, their changed attachment point to the Internet must be reflected in the inter-domain routing system and BGP needs to update the routing tables worldwide. This leads to an increased BGP signalling rate, fragmented IP number space, and increased BGP routing tables.

The locator/identifier (Loc/ID) split principle is expected to overcome the presented problems and, in particular, scaling issues in the Internet [1], [2]. It works as follows: Full addresses consist of two parts: the ID identifies an endpoint and the Loc describes its location in the Internet. Applications know only IDs and send packets to destination IDs. When a packet is sent to an ID, a mapping system is needed to provide the corresponding Loc for the ID. The Loc is added to the packet and used for forwarding the packet in the Internet. The mapping system must be resilient to outages, secure, and fast as it is a vital part of an Internet based on the Loc/ID split. When the location of an ID changes, the mapping system is updated with the new ID-to-Loc information. Neither endpoint renumbering nor changes to the routing system are needed to make the ID reachable at the new location.

A few routing proposals add the Loc at the source node [3], [4], but many others add it at some intermediate node [5]–[11]. In the latter case, packets are already on the way when the Loc information needs to be added. This is a special challenge when the mapping information is not yet available at this node. One option is to relay such packets over the mapping system to the destination. The Domain Name System (DNS) is a powerful mapping system, but it is not designed to relay packets.

In this work, we present FIRMS, a distributed mapping system for future Internet routing. It supports routing architectures implementing the Loc/ID split. It is fast, scalable, resilient, secure, and it is able to relay packets.

The paper is organized as follows. In the next section, we briefly review the Loc/ID split architecture LISP as we use its nomenclature in the remainder of the paper. Sect. III describes FIRMS in detail and the Sect. IV presents a rough calculation about the expected load on various system components. Sect. V concludes this work.

II. Basics of LISP

The Loc/ID Separation Protocol (LISP) [5] is a new routing architecture implementing the Loc/ID split. It is currently being standardized by the Internet Engineering Task Force (IETF) [12] and pilot networks already exist. LISP divides the IP address range into two subsets. Endpoint identifiers (EIDs) identify end-hosts on a global scale and are used to forward packets inside LISP domains. LISP domains are edge networks that are connected via LISP gateways to the core of the Internet. In the Internet core, only globally routable addresses are used to forward packets. They are called routing locators (RLOCs). The communication between LISP nodes inside the same LISP domain works like in today's Internet. However, the communication between LISP nodes in different LISP domains requires tunnelling. The LISP node in the source domain addresses a packet to its destination EID. The packet is forwarded to the LISP gateway which then acts as an ingress tunnel router (ITR). It queries the mapping system for the RLOC of the gateway that belongs to the LISP domain hosting the destination EID given in the packet. The mapping system returns the desired EID-to-RLOC information to the ITR which then encapsulates the packet towards the obtained RLOC and sends it. The ITR stores the mapping in its local cache to avoid another query for the same EID. The gateway of the destination LISP domain receives the tunnelled packet and acts as an egress tunnel router (ETR). It just strips off the encapsulation header and forwards the packet according to the destination EID which is routable in the destination LISP domain. Interworking techniques with the non-LISP Internet are described in [13].

Manuscript received 8 November 2009; revised 11 June 2010. This work was funded by the Federal Ministry of Education and Research of the Federal Republic of Germany (support code 01 BK 0800, G-Lab). The authors alone are responsible for the content of the paper.

The authors are with University of Würzburg, Institute of Computer Science, Germany (e-mail: menth@informatik.uni-wuerzburg.de).

Digital Object Identifier 10.1109/JSAC.2010.101010.

0733-8716/10/$25.00 © 2010 IEEE

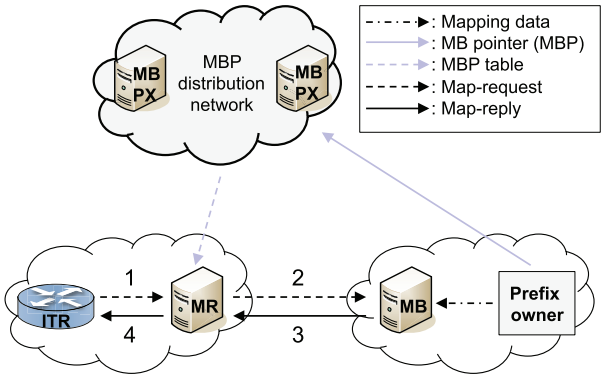

Fig. 1. Basic operation of FIRMS.

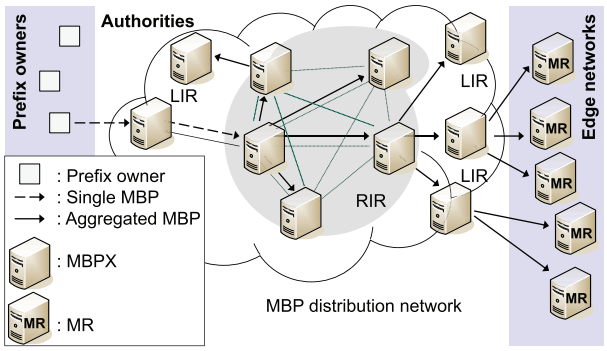

Fig. 2. Propagation of MBP updates in the map-base pointer distribution network.

III. The FIRMS Architecture

In this section we present FIRMS, a new mapping system for future Internet routing. We describe its architecture, specify its operation, and discuss its resilience and security features. We make use of LISP's nomenclature (EID, RLOC, ITR, ETR), but FIRMS is also applicable to other routing approaches that are based on the Loc/ID split.

A. General Idea

Fig. 1 illustrates the basic structure and operation of FIRMS. We assume that EIDs are assigned to their owners in prefix blocks. Each prefix owner provides a map-base (MB) holding the EID-to-RLOC mappings for all its EIDs. The operation of the MB may be delegated to a specialized company. A map-base pointer (MBP) is a data structure containing information about the MB. The prefix owner registers this information in the global MBP distribution network which collects all MBPs and constructs a global MBP table. Each ITR is configured with a map-resolver (MR). The MR registers at the MBP distribution network and receives a copy of the global MBP table. When the ITR requires an EID-to-RLOC mapping for an EID, it sends a map-request to its MR. The MR looks up the address of the responsible MB in its local copy of the MBP table and forwards the map-request to that MB. The MB returns a map-reply containing the desired EID-to-RLOC mapping to the MR which forwards it to the ITR. If a non-existing mapping is queried, a negative map-reply is returned. This design requires that MRs and MBs have globally reachable RLOC addresses. We present ITRs and MRs as two different entities because they have different functionality. However, the MR functionality may be integrated in an ITR which saves communication overhead and simplifies the design.

B. Map-Base Pointer Distribution Network

We explain how MBPs are distributed from prefix owners to MRs. We assume that EIDs are assigned in a similar way as IP addresses are assigned today; many routing proposals even assume that EIDs are IP addresses. IANA delegates IP address blocks to the five regional Internet registries (RIRs): AfriNIC, APNIC, ARIN, LACNIC, and RIPE NCC. They delegate subsets thereof to local Internet registries (LIRs). Both RIRs and LIRs partition the address space in prefix blocks and assign prefixes to organizations (prefix owners).

Every RIR or LIR runs a map-base pointer exchange node (MBPX). Fig. 2 shows that the MBPX of a LIR (LIR-MBPX) is connected to the MBPX of its RIR (RIR-MBPX), and the RIR-MBPXs are fully meshed. This constitutes the MBP distribution network. The prefix owner adds, changes, or removes MBPs for its EID prefixes at the MBPX of its LIR or RIR. An LIR-MBPX forwards this data to its superordinate RIR-MBPX. The RIR-MBPX collects the MBPs for all EID prefixes under its control and compiles a regional MBP table. The MBP tables are exchanged among all RIR-MBPXs so that each of them has a copy of the global MBP table. They push this information to their subordinate LIR-MBPXs which forward it to all MRs that have registered for that service. An involvement of RIRs or LIRs for the support of Internet services is not uncommon. For instance, RIRs and LIRs play an active role for reverse DNS lookup.

To facilitate incremental updates to MBP tables, the RIR-MBPX collects individual MBP updates from prefix owners over some time and provides sequentially numbered aggregated updates. It pushes them to the other RIR-MBPXs and its subordinate LIR-MBPXs. When an RIR-MBPX, LIR-MBPX, or MR receives such an update, it applies the changes to its local copy of the MBP table and forwards the updates to all its subordinate LIR-MBPXs or MRs. The numbering of the updates contributes to the consistency of all MBP tables. If an update is received with an unexpected number, missing updates are detected and their retransmission is requested.

C. Mapping Retrieval

To minimize query overhead, ITRs and MRs have local caches for EID-to-RLOC mappings. To avoid stale information, mappings are automatically purged from the caches after their time-to-live has expired. Fig. 3 illustrates how EID-to-RLOC mappings are retrieved in combination with caches. When the ITR requires a mapping, it first checks its cache and can often retrieve the mapping immediately. In case of a cache miss, the ITR sends a map-request to the MR.

When the MR receives a map-request from an ITR, it first searches its cache and, if successful, sends a map-reply back to the ITR. If unsuccessful, the MR searches its local copy of the MBP table using a longest prefix match with the requested EID and selects the appropriate MBP. It chooses a suitable MB from that MBP and sends a map-request to that MB. The MR keeps a state for the requested EID so that a map-reply can

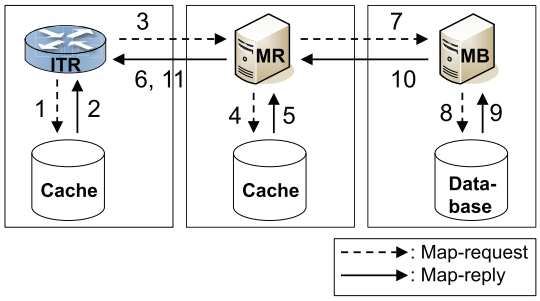

Fig. 3. Cascading mapping retrieval in FIRMS.

later be returned to the requesting ITR. The state is removed when the MR returns the requested information to the ITR or when a timer expires.

When the MB receives a map-request from a MR, it retrieves the EID-to-RLOC mapping from its database and sends it back to the MR in a map-reply. The MR stores the mapping of the map-reply in its cache and sends a map-reply back to the ITR which also stores the mapping in its cache. The caches at the ITRs and MRs minimize the retrieval time for the mappings and reduce the frequency of map-requests. Performance issues of caches have been discussed in [14].

We propose several enhancements to improve the speed and scalability of the mapping retrieval.

- MRs and ITRs should limit the rate of map-requests for the same EID to avoid outgoing map-request storms.
- Every EID may have its own RLOC. If EIDs of a common prefix block share the same RLOC, their EID-to-RLOC mappings may be aggregated to a single EID-prefix-to-RLOC mapping. On the one hand, this saves storage in caches and databases. On the other hand, an EID-prefix-to-RLOC mapping covers the RLOCs for many EIDs. That makes additional map-requests redundant when the ITR needs a mapping for a new EID that is already covered by an EID-prefix-to-RLOC mapping in its cache. Thus, EID-prefix-to-RLOC mappings minimize the lookup delay and take load off the MR and the MB.
- If an MR serves only a single ITR, the caches of the MR and the ITR are likely to have the same content so that advantage cannot be taken from the cache at the MR. Hence, several ITRs should be configured with the same MR. Then, the MR may be able to serve an ITR's map-request from its cache with EID-to-RLOC mappings that have been requested earlier by other ITRs.
- Alternatively, the MR functionality may be integrated in ITRs. This saves communication overhead and simplifies the overall structure. Then, the MR is mainly an interface to logically separate ITR and MR functionality within the same physical node.

D. Packet Relaying

We first outline the motivation for a packet relaying service and then explain how it can be offered by FIRMS.

1) Motivation for Packet Relaying: When an ITR receives a packet addressed to an outbound EID, it tries to retrieve the EID-to-RLOC mapping from its local cache and, if successful, tunnels the packet to the ETR whose RLOC was given in the mapping. In case of a cache miss, the ITR retrieves the mapping over the network which is a time-consuming process. This can happen for the first packet of a communication session when a new flow to a previously not contacted EID is established. The arrival rate of such packets is most likely rather low. In contrast, when traffic is shifted from one ITR to another, the rate of packets with missing RLOCs can be very high. This can happen, for example, when the primary ITR of a networks fails, when the internal routing is changed, or when load balancing policies change. There are three options to handle such outbound packets until their mappings are available in the ITR cache: they can be dropped, stored, or relayed to another node that knows how to forward them.

When the ITR drops packets, many applications will resend them, and by then the mapping is hopefully available in the ITR's cache. This might work for the first packet of a communication, but especially this packet can be quite important, e.g., the initial SYN packet of a TCP connection setup. Losing the first packet can significantly impede the communication setup. When a large number of flows is shifted from another ITR, an immense number of packets is dropped until a mapping can be retrieved from the MS.

As an alternative, the ITR stores the packet until the requested mapping returns from the MR. Then, the ITR can add the RLOC to the packet and send it. This option requires a large buffer to store such packets. Additional logic is needed to continue the processing of the packets as soon as the missing mappings arrive or to drop them when a timer expires. The buffer may overflow and packets may be lost, especially when packets arrive at a high rate. This gives rise to potential attacks where attackers send packets to the ITR with yet unknown destination EIDs. Thus, this option requires complex engineering and still cannot avoid packet loss.

Packet relaying to another node that knows how to forward the packet seems a promising idea because it avoids the drawbacks of dropping and storing. Therefore, it has been proposed also for other mapping systems in the LISP context under the name "data probe" [15]–[17].

2) Packet Relaying in FIRMS: Fig. 4 illustrates how packet relaying can be realized in FIRMS. Normally, the ITR has the EID-to-RLOC mapping in its cache and tunnels the packet to the ETR. In case of a cache miss, the ITR tunnels the packet to the MR. If the MR finds the required mapping in its cache, it tunnels the packet to the ETR. Otherwise, the MR tunnels the packet to the appropriate MB. The MB has the mapping in its database and tunnels the packet to the ETR. This design has several nice properties.

- Only the MR and the MB are involved in the relay process. They are operated by the sender's network and the prefix owner or on behalf of the prefix owner so that these elements have economic incentives to forward the data. In particular, no elements of public infrastructure or other private networks are involved. This is different in other proposals where relayed packets are transmitted over an overlay network [15]–[17].
- If the MB is collocated with the destination network of the EID and near the ETR, the path of the relayed packets is hardly stretched.
- Relayed packets can be interpreted as implicit map-

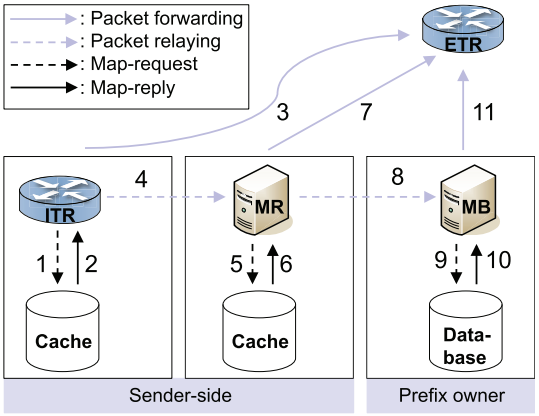

Fig. 4. Packet forwarding and relaying in FIRMS.

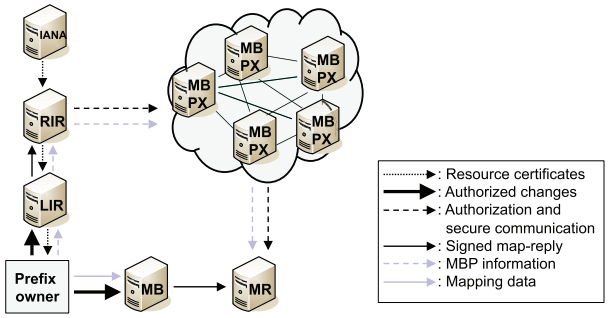

Fig. 5. Security concept for FIRMS.

requests and save explicit map-requests. That means, MRs or MBs not only tunnel the relayed packets to ETRs when they have appropriate mappings, they also respond with map-replies. When an ITR relays multiple packets with the same EID, map-reply storms may occur and measures should be taken to avoid them (see Sect. III-C).

E. Resilience Concept

We propose a protection concept for FIRMS based on simple replication so that the mapping service survives in case of any component failure. Moreover, additional LISP-specific resilience methods can also be applied with FIRMS.

1) Protection for FIRMS: RLOCs can become unreachable. If an edge network is multihomed, it is reachable over alternative RLOCs that also appear in the EID-to-RLOC mappings. When an ITR detects problems with an RLOC, it marks the particular RLOC in its cache as unreachable for a while and uses an alternative RLOC instead.

MRs can fail. ITRs can be configured with multiple MRs. When an ITR detects the failure of an MR, it marks the MR as unreachable for a while and contacts another configured MR.

MBs can fail. A prefix owner has multiple MBs with identical mappings and records their addresses in the MBP. When an MR detects the failure of an MB, it marks the MB as temporarily unreachable and contacts an alternative MB whose address is given in the MR's local copy of the MBP table.

MBPXs can fail. As a consequence, MRs do not receive updates for the MBP table in time. An MR can register with multiple MBPXs, and if one of them fails, the MR still receives updates from the other MBPXs.

2) LISP-Specific Protection: The LISP encapsulation header reserves four bytes as "locator status bits" [12]. These bits correspond to an ordered list of RLOCs in the EID-to-RLOC mapping and indicate which of them are operational. The prefix owner can change this information at the MBs to give the ITRs a hint which RLOCs are currently reachable.

In addition, database map-versioning is proposed. EID-to-RLOC mappings are equipped with version numbers to facilitate detection of outdated information. The ITR adds the current version number for the mapping of the source EID in the LISP encapsulation header. The ETR examines the version number in the encapsulation header of incoming packets and compares them with the version number in the corresponding mappings stored in the local cache of the collocated ITR. If the mapping in the local cache is outdated, the ITR sends a map-request for the respective EID to update the mapping in its cache. This mechanism helps to keep track of mapping changes.

F. Security Concept

In Loc/ID split based routing architectures it is crucial that EID-to-RLOC mappings are recent and authentic. In FIRMS, MBs are under the control of prefix owners who must make sure that their MBs respond with correct mappings for their EID range. The MR must be able to verify that mappings arrive from the queried MB, and that mappings are unaltered and recent, e.g., that they are not a replay of an old mapping entry. We first propose mechanisms which ensure that the MR can trust the information in its MBP table, and then we add functionality to achieve the other requirements.

Fig. 5 visualizes the security concept of FIRMS. In [18] an extension to the ITU-T X.509 v3 standard for a public key infrastructure (PKI) has been proposed that allows to bind a list of IP prefixes to the subject of a so-called resource certificate. It is already provided for use by APNIC [19]. We use it in FIRMS to transfer the right-to-use for IP prefixes from IANA through the RIRs and LIRs to prefix owners. Thus, prefix owners can authenticate themselves as the rightful owners of their EID prefixes. They use this feature for adding, modifying, or removing EID-to-RLOC mappings at the MBs, and for adding, modifying or removing MBPs at the MBPX of the LIRs/RIRs from which they received their EID space.

When MBP updates are propagated from subordinate MBPXs to superordinate MBPXs, transport layer security (TLS) [20] or datagram TLS (DTLS) [21] together with resource certificates ensure that an MBPX can propagate MBP changes over a secured connection only if it has the the right-to-use for the corresponding EID ranges. The MBPX of an LIR trusts the MBPX of its RIR or superordinate LIR, and each MR trusts the MBPXs it is connected to. To receive trusted MBP updates from them, they just authenticate them and use a secured connection for data transport. As a result, the MR can trust the MBP information in its local MBP table.

A MR must be able to verify whether the mappings obtained from an MB are authentic and recent. To that end, an additional PKI for MBs is introduced. The MB includes a

time stamp in the map-reply and signs the map-reply with its private key before sending the map-reply to the MR. The public key of each MB is included in the the corresponding entry of the global MBP table whereof each MR already stores a local copy. When the MR receives a map-reply, it uses the MB's public key to validate the message to be sure that the contained mapping is authentic, and checks the time stamp to be sure that the mapping is recent. The MR can immediately validate the obtained map-replies without verifying any trust chain which would generate extra delay and traffic. This was a major design goal of the FIRMS architecture and ensures that FIRMS is fast and scalable.

G. Comparison of FIRMS with Other Approaches

LISP assumes that MBs are collocated with ETRs. To make the LISP specification independent of a specific mapping system, LISP-Map-Server [22] defines a map-resolver interface for ITRs and a map-server interface for ETRs so that the way how map-requests find the appropriate MB, i.e., the specific mapping system, can be exchanged. Currently, LISP+ALT [15] is the preferred mapping system. It defines a semi-hierarchical overlay structure over which map-requests from the ITR are forwarded to the appropriate ETR in an efficient way. LISP-DHT [23] uses a distributed hash table for that purpose. The structure of LISP-TREE [24] is similar to the one of the DNS system. In [25], we propose a classification of mapping systems and compare FIRMS with many others in detail.

IV. Performance Analysis

In this section we estimate the expected loads on various system components in FIRMS and show that they are in a manageable order of magnitude.

A. Record Sizes

We calculate the size of EID-to-RLOC and MBP records in FIRMS. We assume that both EIDs and RLOCs have the same format as IPv6 addresses which are 16 bytes long. Edge networks can take advantage of multihoming more easily with Loc/ID split, but being connected to more than 4 ISPs has only limited benefit [26]. Therefore, we assume that nodes are usually connected to the Internet over three providers which results in an average number of three RLOCs per EID-to-RLOC record. This record contains additional information like a time-to-live (5 bytes), some traffic engineering attributes (10 bytes), and a security signature with a timestamp (16+5 bytes) so that its average size is about 100 bytes.

MBPs consist of an EID prefix (8 bytes), the RLOCs (16 bytes each) and public keys (64 bytes each) of the corresponding MBs, and some additional attributes for traffic engineering (10 bytes). For resilience and load balancing purposes, each EID prefix should have two separate highly available MBs so that we assume two MBs per MBP. This sums up to an average size of 178 bytes per MBP record.

B. Storage Requirements

We estimate the storage requirements of a MB and for the MBP table in FIRMS. The current number of prefixes in the Internet is about $n_{pref} = 10^6$ [27] while the current number of hosts is about 10^9 [28]. This leads to an average number of $n_{pref}^{EIDs} = 10^3$ hosts per prefix. With the Internet of things and other novel applications, we assume that the number of hosts (and EIDs) per EID prefix will dramatically increase in the future. The same holds for the number of EID prefixes.

A MB needs to store on average $n_{pref}^{EIDs} = 10^3$ EID-to-RLOC mappings (100 Kbyte) today and a multiple of them in the future. That does not seem a critical value. The MBP table keeps $n_{pref} = 10^6$ MBP entries (178 Mbyte) and a multiple in the future. Also that seems feasible.

C. Update and Map-Request Loads

We calculate the update load in a MB and for the MBP table in FIRMS. The MB provider may be independent of the ISP of a network. In that case, a customer may change its ISP while keeping its MB provider. Thus, the validity of a MBP can outlast the contract between a customer network and an ISP. A recent study showed that only 32 percent of small and medium companies changed their provider in 2008 [29]. Thus, we assume that prefix owners change their MBPs every 3 years which also includes key updates for the MBs. With 10^6 prefixes, this leads to an average update rate for MBPs of 38 prefixes or 6.77 Kbytes per hour. Also a much larger multiple seems quite feasible in particular as MBP updates are aggregated and not sent individually as this rough calculation assumes. RIRs have between 1000 and 6500 subordinate LIRs. Hence, they need to push 1.05 Gbytes daily towards their LIRs. This is a large amount of data but breaks down to a continuous upload rate of 12.2 Kbytes/s so that even a large multiple is feasible.

EID-to-RLOC mappings are less stable when nodes become increasingly mobile. We assume that an EID changes its mapping once a month. This is rather an average over all nodes than a typical value since some devices are significantly more mobile than others. A MB in FIRMS which is responsible for a single EID prefix with 10^3 EID-to-RLOC mappings encounters 33 updates per day. This is more than feasible even if a MB stores the mappings for multiple EID prefixes and if the number of EID is orders of magnitude larger.

With FIRMS, the worldwide request load is not problematic since a MR handles only the load originating at an ITR and the MB handles only the request load for a single or a few EID prefixes.

D. Resolution Delay

The resolution delay with FIRMS is rather small. The mappings for most packets are available in the local cache. In case of a cache miss, the MR of the source network queries the MB which should be located in a well accessible place in the Internet. When the map-reply returns, the MR can immediately validate the authenticity of the received data and forward it to the ITR for further use. Thus, FIRMS is rather fast as the resolution delay consists essentially of round trip time to the MB, assuming that local operations are fast.

V. Conclusion

New routing architectures implementing the Loc/ID split have been proposed for the Internet. In many of them, an intermediate node queries a mapping system for ID-to-Loc mappings. We have presented FIRMS for that purpose. It includes security and resilience features and can relay packets when intermediate nodes encounter cache misses for required ID-to-Loc mappings. Our performance analysis showed that storage requirements, update loads, and resolution delays for FIRMS are manageable. We have implemented a proof-of-concept for FIRMS in the G-Lab experimental facility and demonstrated its operation [30].

Acknowledgements

The authors thank Phuoc Tran-Gia for the support by G-Lab, Scott Brim, Anja Feldmann, David Hock, Dominik Klein, Tony Li, Wolfgang Mühlbauer, Tim Neubert, Steve Uhlig, Christian Vogt, Lixia Zhang for valuable input and stimulating discussions.

References

[1] D. Meyer, L. Zhang, and K. Fall, "RFC4984: Report from the IAB Workshop on Routing and Addressing," Sep. 2007.

[2] B. Quoitin, L. Iannone, C. de Launois, and O. Bonaventure, "Evaluating the Benefits of the Locator/Identifier Separation," in *ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch)*, Kyoto, Japan, Aug. 2007.

[3] R. Atkinson, S. Bhatti, and S. Hailes, "ILNP: Mobility, Multi-Homing, Localised Addressing and Security through Naming," *Telecommunication Systems*, vol. 42, no. 3–4, pp. 273 – 291, Dec. 2009.

[4] A. Feldmann, L. Cittadini, W. Mühlbauer, R. Bush, and O. Maennel, "HAIR: Hierarchical Architecture for Internet Routing," in *Re-Architecting the Internet (ReArch)*, Rome, Italy, Dec. 2009.

[5] D. Meyer, "The Locator Identifier Separation Protocol (LISP)," *The Internet Protocol Journal*, vol. 11, no. 1, pp. 23–36, Mar. 2008.

[6] C. Vogt, "Six/One Router: A Scalable and Backwards Compatible Solution for Provider-Independent Addressing," in *ACM International Workshop on Mobility in the Evolving Internet Architecture (MobiArch)*, Seattle, WA, USA, Aug. 2008.

[7] D. Jen, M. Meisel, D. Massey, L. Wang, B. Zhang, and L. Zhang, "APT: A Practical Tunneling Architecture for Routing Scalability," UCLA Computer Science Department, Tech. Rep. 080004, Mar. 2008.

[8] O. Hanka, C. Spleiss, G. Kunzmann, and J. Eberspächer, "A Novel DHT-Based Network Architecture for the Next Generation Internet," in *International Conference on Networking (ICN)*, Mar. 2009.

[9] S. Schuetz, R. Winter, L. Burness, P. Eardley, and B. Ahlgren, "Node Identity Internetworking Architecture," http://tools.ietf.org/id/draft-schuetz-nid-arch-00.txt, Sep. 2007.

[10] X. Xu, "Routing Architecture for the Next Generation Internet (RANGI)," http://tools.ietf.org/id/draft-xu-rangi-02.txt, Jul. 2009.

[11] M. Menth, M. Hartmann, and D. Klein, "Global Locator, Local Locator, and Identifier Split (GLI-Split)," University of Würzburg, Institute of Computer Science, Technical Report, No. 470, Apr. 2010.

[12] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "Locator/ID Separation Protocol (LISP)," http://tools.ietf.org/html/draft-ietf-lisp, Apr. 2010.

[13] D. Lewis, D. Meyer, D. Farinacci, and V. Fuller, "Interworking LISP with IPv4 and IPv6," http://tools.ietf.org/html/draft-ietf-lisp-interworking, Mar. 2010.

[14] L. Iannone and O. Bonaventure, "On the Cost of Caching Locator/ID Mappings," in *ACM Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, Dec. 2007.

[15] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "LISP Alternative Topology (LISP+ALT)," http://tools.ietf.org/html/draft-ietf-lisp-alt, Mar. 2010.

[16] S. Brim, N. Chiappa, D. Farinacci, V. Fuller, and D. Lewis, "LISP-CONS: A Content distribution Overlay Network Service for LISP," http://tools.ietf.org/html/draft-meyer-lisp-cons, Apr. 2008.

[17] S. Brim, D. Farinacci, D. Meyer, and J. Curran, "EID Mappings Multicast Across Cooperating Systems for LISP," http://tools.ietf.org/html/draft-curran-lisp-emacs-00, Nov. 2007.

[18] C. Lynn, S. Kent, and K. Seo, "RFC3779: X.509 Extensions for IP Addresses and AS Identifiers," Jun. 2004.

[19] G. Huston, "Resource Certification," *The Internet Protocol Journal*, vol. 12, no. 1, pp. 13–26, Mar. 2009.

[20] T. Dierks and E. Rescorla, "RFC5246: The Transport Layer Security (TLS) Protocol Version 1.2," Aug. 2008.

[21] E. Rescorla and N. Modadugu, "RFC4347: Datagram Transport Layer Security," Apr. 2006.

[22] D. Farinacci and V. Fuller, "LISP Map Server," http://tools.ietf.org/html/draft-ietf-lisp-ms, Apr. 2010.

[23] L. Mathy and L. Iannone, "LISP-DHT: Towards a DHT to Map Identifiers onto Locators," in *Re-Architecting the Internet (ReArch)*, Madrid, Spain, Dec. 2008.

[24] L. Jakab, A. Cabellos-Aparicio, F. Coras, D. Saucez, and O. Bonaventure, "LISP-TREE: A DNS Hierarchy to Support the LISP Mapping System," *accepted for IEEE J. Sel. Areas Commun.*, 2010.

[25] M. Menth, M. Hartmann, and M. Hoefling, "Mapping Systems for Loc/ID Split Internet Routing," University of Würzburg, Institute of Computer Science, Technical Report, No. 472, May 2010.

[26] A. Akella, B. Maggs, S. Seshan, A. Shaikh, and R. Sitaraman, "A Measurement-Based Analysis of Multihoming," in *ACM SIGCOMM*, Karlsruhe, Germany, Aug. 2003.

[27] RIPE NCC, "RIS Statistics Report," http://www.ris.ripe.net/weekly-report/, 2009.

[28] Internet System Consortium, "The ISC Domain Survey," https://isc.org/solutions/survey, 2009.

[29] P. Martin, "Zen Internet UK Small Medium Enterprise (SME) survey," Shape the Future Limited, Tech. Rep., Nov. 2008.

[30] M. Hartmann, D. Hock, M. Hoefling, T. Neubert, and M. Menth, "Demonstration of the Future InteRnet Mapping System (FIRMS) in the G-Lab Experimental Facility," *Wuerzburg Workshop on IP: Visions of Future Generation Networks (EuroView)*, Aug. 2010.

Michael Menth studied computer science and mathematics at the Univ. of Wuerzburg/Germany and Austin/Texas. He worked at the Univ. of Ulm/Germany and Wuerzburg and obtained his Ph.D. in 2004. Since then, he is assistant professor and leads a research group on future Internet. His special interests are performance analysis, optimization of communication networks, resource management, as well as routing and resilience issues. Dr. Menth holds numerous patents and received various scientific awards for innovative work.

Matthias Hartmann studied computer science and mathematics at the University of Wuerzburg/Germany, the University of Texas at Austin, and at the Simula Research Laboratory in Oslo/Norway. He received his Diploma degree in computer science in 2007. Currently, he is a researcher at the Institute of Computer Science in Wuerzburg and pursuing his Ph.D. His current research focuses on performance and resilience analysis as well as on future Internet routing.

Michael Höfling studied computer science and physics at the University of Wuerzburg/Germany and computer science at the University of Umeå/Sweden. He received his B.Sc. and M.Sc. degree in computer science from the University of Umeå/Sweden in 2008, and his German diploma in computer science from the University of Wuerzburg in 2010. His current research focuses on future Internet addressing and routing.