HiiMap: Hierarchical Internet Mapping Architecture

Oliver Hanka, Christoph Spleiß, Jörg Eberspächer
Technische Universität München
oliver.hanka, christoph.spleiss, joerg.eberspaecher@tum.de

1. Introduction

Many researchers working on concepts for the Next Generation Internet agree that the split of locator and identifier seems a very promising approach. Although this solution addresses the most critical issues in todays internet, like the shortage of available addresses and no support for mobility, new challenges arise through the mapping between the locator and the identifier. As the mapping service is involved in the setup of *every* communication it has to cope with high query rates. Therefore, DHTs seem to be a promising solution to provide scalability and load balancing to the mapping service. However, trust and security problems arise because of the storage location of a locator-identifier pair is likely to be random over all participating members.

HiiMap presents a new Internet Architecture based on a locator/identifier split with a special focus on the trust problem of DHT-based mapping services. With administrative regions that handle mapping requests and a central authority for the resolution of mapping regions, this approach covers all critical issues of the current internet while still considering trust and security.

2. Terms and definitions

UID: The *Unique Identifier* is a flat, randomized and world-wide unique address assigned for lifetime to a node. It corresponds with the identifier in the locator/identifier split architecture. The UID is used to identify a node or user, but is not routable.

LTA: The *Local Temporary Address* is one part of the locator of each node. It is assigned by a provider to its customer and is routable in the provider's own network or autonomous system (AS). Together with the address of the Border Gateway Router, the Gateway UID (gUID) that specifies an entrance point into the network, the LTA builds the locator. Hereby, any node can be addressed from any point in the internet. The addressing scheme for the LTA is arbitrary and can be of any kind (e.g. IPv4 or IPv6). Whenever a node changes its access point to the internet, it is assigned a new LTA and maybe also a new gUID.

Mapping: An integral part of any locator/identiefier architecture. The mapping must be able to resolve the current valid locator to a given UID. As mobility is one benefit of a locator/identifier split architecture, the mapping system must be able to cope with a high update frequency of locators due to mobility of nodes. It must be also able to handle very high query rates, as it is involved in every communication setup.

3. HiiMap concept

Some proposals suggest using a global DHT for the mapping service where each provider participating in the internet is a part of. Because of security problems mentioned before and the fact that a centralized database would not be able to handle the mapping of the whole internet, HiiMap suggests the introduction of mapping regions and an additional *Global Authority (GA)*. Thereby, each region has its own independent mapping system which is responsible for the mapping of identifiers of nodes residing in this region. We suggest that each country builds up a region because we have a common legal system among the participating providers. It is up to the region if the mapping system is organized as a DHT or as a centralized database.

In order to resolve the region which is responsible for a specific identifier, a *region prefix (RP)* to any UID is introduced. If the RP is not known, it can be resolved by querying the GA. Thereby, the GA does not return the locator, but only the responsible region. Resolved RPs for UID are cached on the client side, so ideally the GA must be queried only if a specific UID moves permanently to another region (relocation) or if a yet unknown UID wants to be contacted. If a node roams temporarily to a different provider, its native region is still responsible for the mapping. This can be compared to the home location register in GSM. Location updates during an existing connection can be signaled in-band resulting in an seamless connection handover.

4. Security and Trust

As we have a GA which is responsible for the region resolution, each region must trust this GA. We suggest to make the GA part of the United Nations, which almost all countries are part of and can therefore trust this authority. Besides this, each UID can generate a public/private key pair, where the public key is part of the mapping entry which is stored in a region. With this, integrity, authenticity and cryptography can be provided.