A Flexible Abstraction for the Future Internet

Florian Liers, Thomas Volkert, Andreas Mitschele-Thiel
{ florian.liers | thomas.volkert | mitsch }@tu-ilmenau.de
Technische Universität Ilmenau

1. Introduction and Motivation

Like the FIND initiative in the US, several EU projects are working at the development of new and revolutionary approaches for a new Internet. The European technology platform eMobility deals especially with the wireless specific issues. Its main design goals are an integrated functional design, the decoupling of interfaces, IDs, addressing scheme and routing. Furthermore several security functions are included. The EIFFEL think tank, an EU support action, stimulates the discussion in the research community. They published recommendations, guidelines and design goals for a new Internet. Their most important objectives for a future Internet protocol are: openness, "wide-scale accessibility, application neutrality, transparency and generic purpose". Furthermore they demand for a decoupling of addressing from "application identification and user identification/location". In combination with research results, published by the US project NewArch, some common key aspects for a future Internet can be extracted:

1. Separation of location, addressing and routing
2. Support of heterogeneous subnetworks or autonomous subsystems with different lower layer techniques and the support of heterogeneous transport layers and applications, respectively.
3. Despite the adherence of the NewArch project to the end-to-end argument, research in the EU tends towards an Intelligent Network approach. Due to the strong focus on mobility, the eMobility platform prefers an Intelligent Network with built-in functions supporting QoS, mobility and security.

Up to now, every new architecture for an Internet either followed the end-to-end argument or the Intelligent Network approach. Most source routing architectures tend to follow the end-to-end arguments. Obviously, enhancing the source route with all information, needed for forwarding a packet, reduces the states needed inside the network to zero. In contrary, flow-oriented approaches are using state information within the network to forward the traffic.

2. Basic Idea

Our idea is to delay the choice between an end-to-end network and an Intelligent Network until the operation phase of a network. Therefore, our architecture enables all modes and a mix of them in a single network. Our proposed architecture will enable the modular injection of intelligent parts. If special intelligence e.g. for efficient multicast is needed, it should be possible to inject exactly the intelligence needed for this function. However the internal mode of operation of a (sub-) network should not be visible outside. Furthermore, a backbone provider should be able to run its network as a dumb end-to-end network with fast packet processing.

3. Our Approach

Our approach extends forwarding-based architectures by introducing an abstract structure for data forwarding consisting of "gates". A gate encapsulates the functionality of the network like a facade, that can implement several functionalities like lower layer functions (IP, MAC), mobility, QoS and others. Packets are used as data inputs for these gates. In summary, we trade in the storage of local connectivity information for a gain in flexibility and security. The basic forwarding-based architecture enables the separation of location, addressing and routing. Hence, by using our approach, a network route is represented by a list of gates which have to be passed by packets. The list of gates has to be determined before each transmission by the sender of a packet with the help of the architecture integrated overlay network of routing services. As answer of a request, a routing services delivers a list of gate identifiers which is used for source routing. During the packet forwarding, each intermediate node removes all elements which addresses locally existing gates from the list and delegates the processing to the local gates corresponding to the removed gate identifiers. The thereby used overlay network of routing services relies on states within the network elements representing the direct neighbors of an element. The architecture allows the introduction of more states (e.g. for flows) if needed. Due to the restriction to local neighborhood information and due to the possibility to have nodes without routing information, the system scales linearly with the total number of nodes attached to the network. Furthermore, the architecture was developed having network security in mind. Therefore, authentication was integrated into the system and it is available for all layers and elements of the network. It is based on the used source routing where signatures are included and the fact that every intermediate entity is able to add its own signature to the packet. Our orthogonal approach for integrating authentication enables an out-of-the-box autonomous network management and optimization unknown for today's networks. It can be used to install flexible policies, which provide a larger design space.