Trust-by-Wire for Packet-switched IP Networks: Tools and FPGA-Prototype for the IPclip System

Peter Danielis, Stephan Kubisch, Harald Widiger,
Jens Schulz, Christian Lange, Dirk Timmermann
University of Rostock
Institute of Applied Microelectronics and Computer Engineering
18051 Rostock, Germany
Tel./Fax: ++49 381 498-7272 / -1187251
Email: {peter.danielis;dirk.timmermann}@uni-rostock.de
Web: http://www.imd.uni-rostock.de/networking

Thomas Bahls, Daniel Duchow
Nokia Siemens Networks
Broadband Access Division
17489 Greifswald, Germany
Tel./Fax: ++49 3834 555-642 / -602
Email: {thomas.bahls;daniel.duchow}@nsn.com

***Abstract*—The packet processing system IPclip (IP Calling Line Identification Presentation) is presented. It is implemented on an FPGA board and configurable at runtime via a graphical configuration tool. The functionality is demonstrated in a localization scenario using an analysis tool and Google Earth.**

I. Introduction

During the last decades, the Internet has steadily developed into a mass medium. On the one hand, newfangled services replace traditional ones. Naturally, these are thereby expected to offer at least the same features as their classical pendants, e.g., when VoIP replaces traditional fixed line telephone networks. On the other hand, the requirements on network infrastructures and services have changed. A reason for that is the lack of the so-called Trust-by-Wire (TBW) in packet-switched IP networks. With TBW, we describe a direct interrelationship between some flavor of user-ID, e.g., a network address, login name, or phone number, and the physical line or geographic location of that user. In other words, TBW stands for unambiguousness and trustworthiness in telecommunication networks. In traditional telephone networks, a phone number directly coheres with a physical line. This direct relationship is not given in modern packet-switched IP networks. An IP address does not identify a physical line! To solve this problem, a new mechanism has been developed, which guarantees TBW in packet-switched IP networks—called Internet Protocol-Calling Line Identification Presentation (IPclip). Already in the access network, unambiguous and trustworthy location information (LI) is added on the IP level.

In modern network applications and especially in access networks, the demands towards functionality and throughput as well as on security and availability are rising permanently. Currently, important driving forces in the Internet are new transmission technologies [1], the growing number of Internet users, and oversubscription of transmission lines. Furthermore, telecommunication carriers have different and changing requirements concerning the network equipment. Hence, only hardware solutions provide sufficient performance for packet classification, manipulation, and forwarding. Due to their flexibility, FPGAs are widely used as target platform. We developed a working FPGA prototype for a packet processing system (PPS).

Section II presents our IPclip prototype. In Section III, we introduce the configuration tool. The analysis tool is described in Section IV. Section V briefly sketches a localization demonstration scenario before the paper concludes in Section VI.

II. IPclip – The Packet Processing System

The PPS is called IPclip. It is currently designed for a Xilinx Virtex-4 FX20 platform FPGA. IPclip's functional submodules offer mechanisms for MTU adaptation, LI verification as well as adding and removing LI.

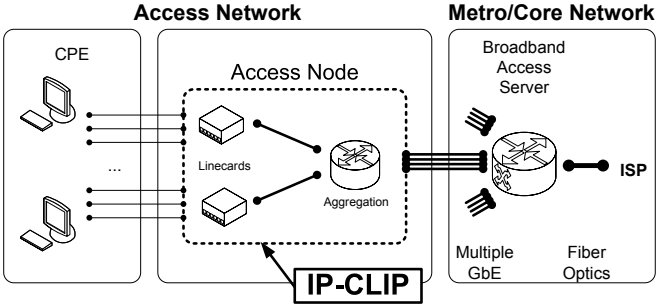

Fig. 1. Access network with IPclip

A. General Functionality

Network ingress—also known as access network—is the most reasonable place where LI can be added and verified. Access networks comprise Customer Premises Equipments (CPEs) as well as so-called access nodes (ANs) like IP DSL Access Multiplexers (IP DSLAMs). Usually, ANs consist of multiple linecards (LCs) and an aggregation card. As sketched in Figure 1, IPclip is located on the LC, which is a trustworthy network element in contrast to CPEs.

With the IPclip mechanism, a customer and his actual geographic location are identified using a tuple, which consists of the current IP address and extra information. While the IP

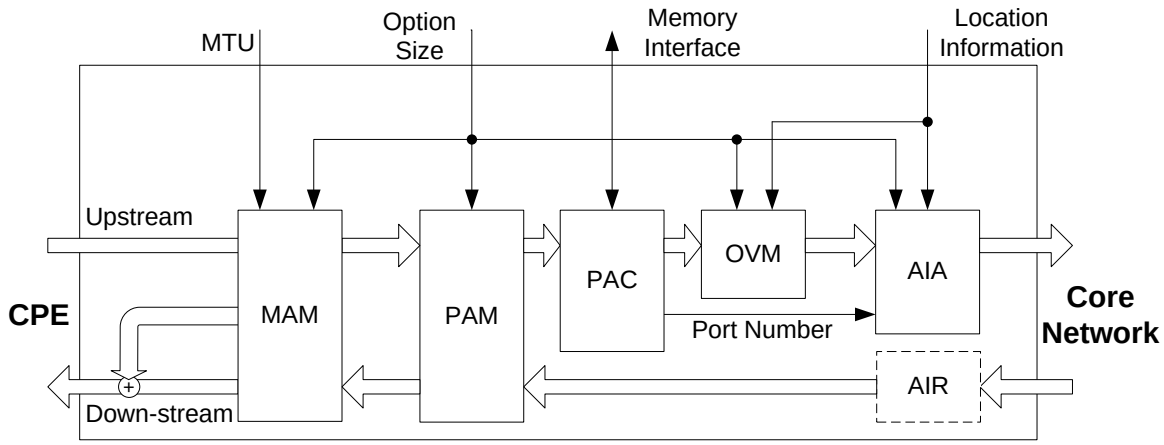

Fig. 2. Internal structure of the IPclip system with serially ordered functional modules

address might identify a user, his position must be part of the additional data. Preferably, a standardized format of LI is used. It can be interpreted for analysis, for classification, for generation of syslog-calls to induce further exceptional actions, or to send help to a person that requires medical assistance in case of VoIP ECs. To provide such LI on a global scale, IPclip inserts it as IP option into every IP packet.

For detailed information on IPclip's functionality and IPclip's use cases, the interested reader is referred to [2], [3].

B. System Architecture

As pictured in Figure 2, IPclip is implemented as a pipelined data path architecture. Communication between the modules bases upon special interfaces. Two main data paths exist within the structure; one upstream path from the customers to the core network and one downstream path. A frame entering the system through the FPGA's internal MACs is first stored in a synchronization buffer for reasons of clock domain crossing. The frame is then forwarded to IPclip's functional modules.

IPclip comprises the functional modules MTU Adaptation Module (MAM), PPPoE MTU Adaptation Module (PAM), Option Verification Module (OVM), Packet Classifier (PAC), Additional Information Adder (AIA), and optionally Additional Information Remover (AIR). MAM carries out the adaptation of the MTU (configurable at runtime) for IPoE. PAM intervenes with the MTU negotiation in case of PPPoE. PAC maps port numbers to every IP packet. OVM identifies and verifies user provided LI by comparing it with LI of the AN. The insertion of LI is done by AIA if the *add*-signal is set. Optionally, AIR can be inserted into the downstream to remove IP-CLIP options from incoming packets.

The modules are serially linked. Finally, the last module forwards the frame to the egress MAC via another synchronization buffer. The basic data flow is the same for up- and downstream data path. Figure 2 depicts the coarse structure of the IPclip system without the synchronization buffers and MACs. At the ingress and egress ports, the system uses FIFOs for clock domain crossing and packet buffering.

IPclip's current architecture is designed to handle Gigabit Ethernet. A frequency of at least $125\ \mathrm{MHz}$ is required for non-blocking performance. To meet different demands, IPclip is highly configurable at synthesis time, e.g., the actual functional spectrum and many parameters regarding the individual functionalities that cannot be configured at runtime.

III. The Configuration Tool

To configure and update IPclip's internal parameters (e.g., LI of the linecard and the size of LI in bytes) dynamically at runtime, we developed a graphical user interface (GUI), which allows for an easy "push-button" configuration of the entire system. The screenshot in Figure 3 shows the GUI of the tool's latest version. It is developed in C++ using the open source version of Trolltech's Qt [4]. The first tab "Global" of the GUI allows for the configuration of global system parameters. The second tab "Rules" is dedicated to configure ports to be added in addition to LI for a corresponding IP packet.

IV. The Analysis Tool

Additionally, an analysis tool has been developed for the IPclip system (see Figure 4). Like the configuration tool, it is implemented in C++ using the open source version of Trolltech's Qt [4]. When packets are received, those containing LI are highlighted and trustworthiness of received LI is indicated.

Received LI can be pictured on a terrestrial globe using Google Earth (see Figure 5). Furthermore, a logical square is spanned surrounding the AN's own position at the packet's destination. The logical square is represented by green walls in Figure 5. Received LI located inside the walls is considered trusted; otherwise it is untrusted. LI and the graphical representation of the logical square is displayed in Google Earth using the Keyhole Markup Language (KML) [5].

V. The Localization Demonstration Scenario

IPclip is implemented on a Xilinx Virtex4 FX20 development board (ML-405). The prototype we are going to present provides a throughput of 1 Gbit/s in each direction. The

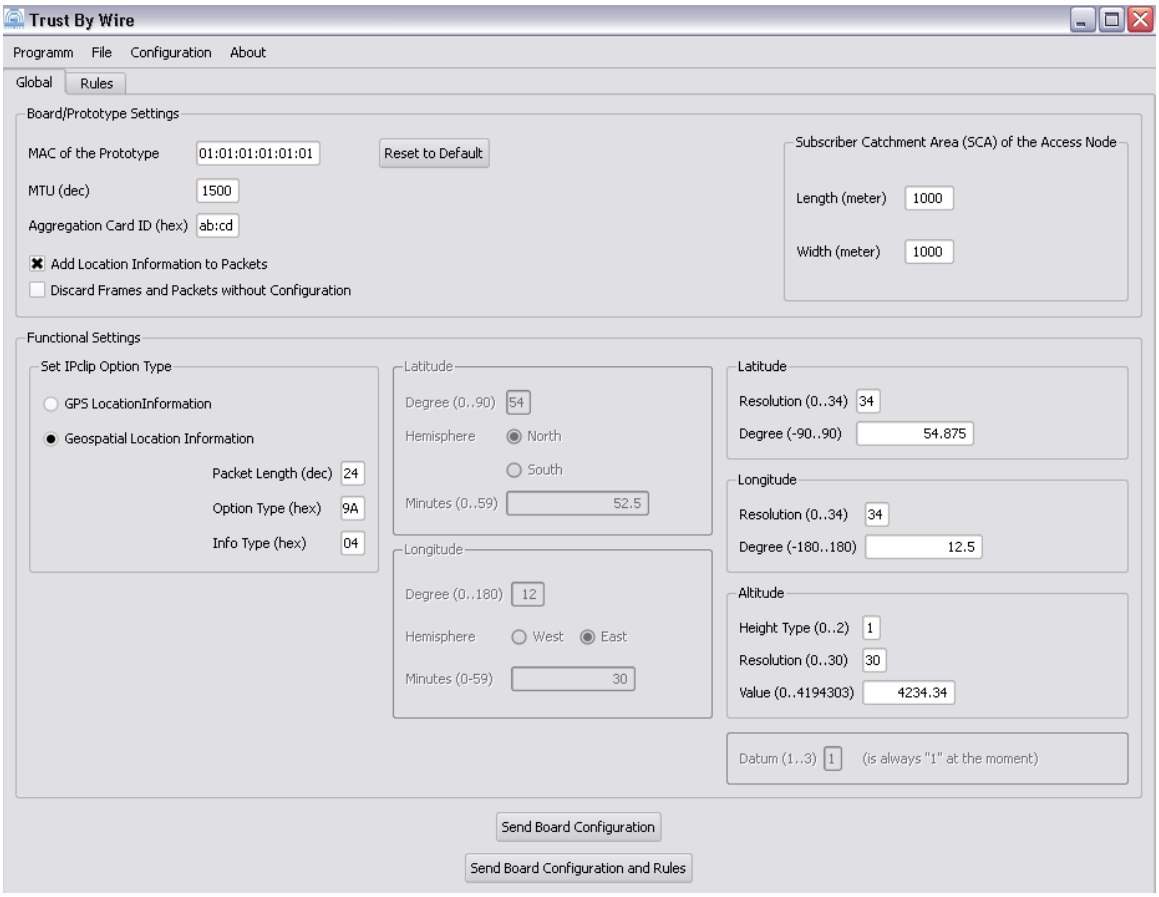

Fig. 3. IPclip configuration tool

typical, complex environment of IPclip on a LC cannot be rebuilt. Instead, a localization demonstration scenario has been prepared, which provides an insight into the operation modi of the different functional modules in the IPclip system.

Localization Demonstration: In this demonstration, a user sends IP packets *without* and *with* LI to a target. Packets without LI are enriched with GPS LI by the FPGA prototype using a GPS receiver. In this case, LI is regarded as network provided, trusted. In packets that contain user provided LI, user provided LI is verified by the IPclip prototype. If user provided LI passes verification, it is labeled as user provided, trusted. Otherwise, user provided LI is replaced by GPS LI and packets are labeled as network provided, untrusted. At the packet's destination, LI is pictured and its trustworthiness is indicated.

VI. Conclusion

We presented the working prototype of the previously published packet processing system called IPclip. For comfortable system configuration, we also proposed a graphical configuration tool, which is used to configure the IPclip prototype on the FPGA development board at runtime. The second GUI serves as an analyzer to picture received location information on a terrestrial globe and to show whether received location information is trustworthy. Furthermore, we briefly introduced a localization demonstration scenario.

Acknowledgment

We would like to thank the Broadband Access Division of Nokia Siemens Networks in Greifswald, Germany for their inspiration and continued support in this project. This work is partly granted by Nokia Siemens Networks.

References

[1] J. Cioffi et al, "Vectored DSLs with DSM: The Road to Ubiquitous Gigabit DSLs," in *Proc. of the World Telecommunications Congress 2006*, Budapest, Hungary, April 30 - Mai 3 2006.

[2] S. Kubisch, H. Widiger, P. Danielis, J. Schulz, D. Timmermann, T. Bahls, and D. Duchow, "Trust-by-Wire in Packet-switched IP Networks: Calling Line Identification Presentation for IP." Genf, Switzerland: 1st ITU-T Kaleidoscope Conference: Innovations in Next Generation Networks - Future Network and Services, 2008.

[3] S. Kubisch, H. Widiger, P. Danielis, J. Schulz, T. Bahls, D. Duchow, and D. Timmermann, "Countering Phishing Threats with Trust-by-Wire in Packet-switched IP Networks - A Conceptual Framework." Miami, FL, USA: 22nd IEEE International Parallel and Distributed Processing Symposium (IPDPS), 4th International Workshop on Security in Systems and Networks (SSN 2008), 2008.

[4] Qt by Trolltech. [Online]. Available: http://www.trolltech.com

[5] KML in Google Earth. [Online]. Available: http://code.google.com/support/bin/topic.py?topic=10426

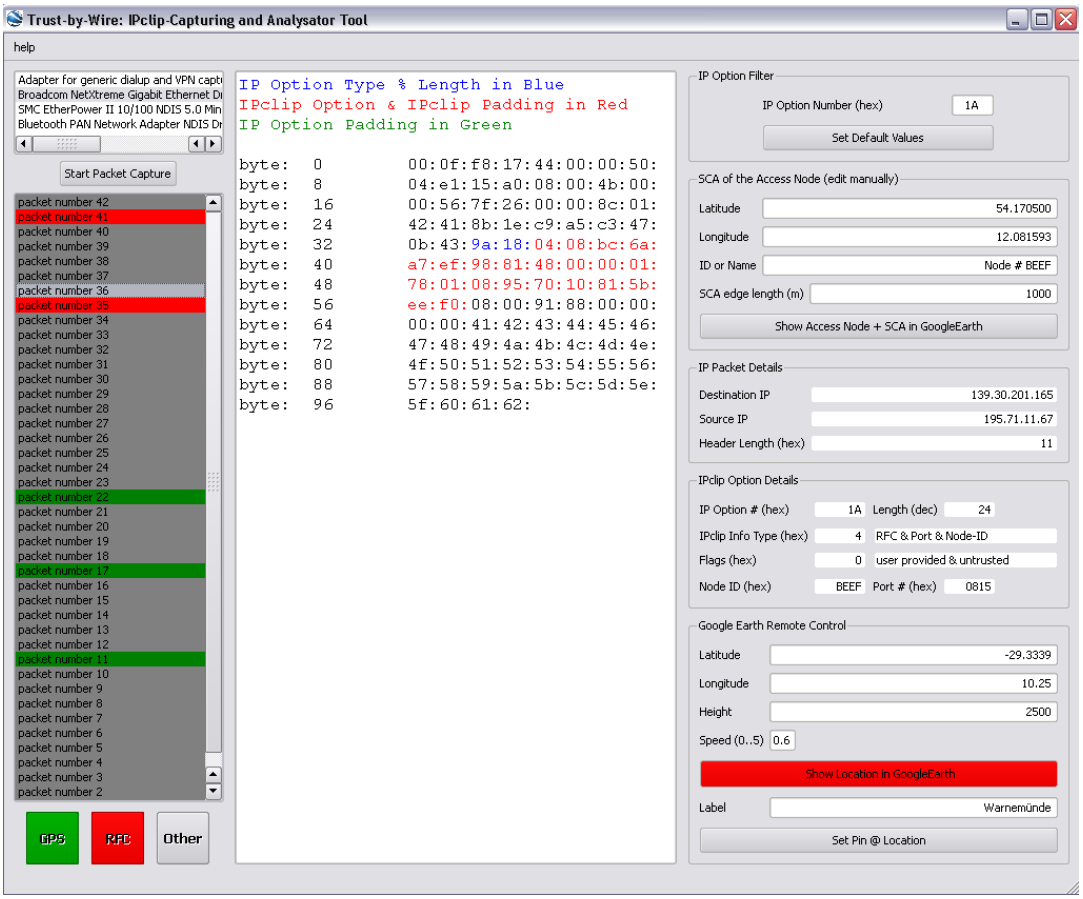

Fig. 4. IPclip analysis tool

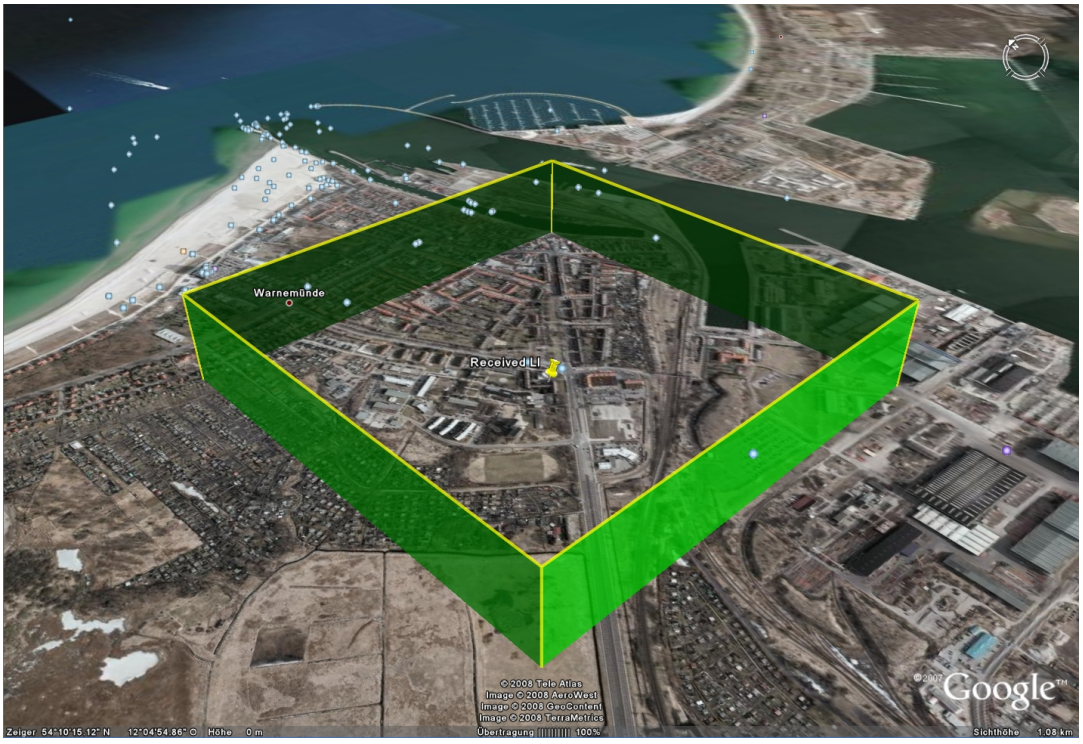

Fig. 5. Received LI in Google Earth