Infocommunications Journal

A PUBLICATION OF THE SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS (HTE)

December 2011 Volume III Number 4 ISSN 2061-2079

PAPERS

SPECIAL ISSUE ON EUROPEAN RESEARCH PROJECTS

ADDITIONAL

Technically Co-Sponsored by

IEEE COMMUNICATIONS SOCIETY

hte

IEEE HUNGARY SECTION

CALL FOR PAPER

8th IFAC Symposium on Biological and Medical Systems

Budapest, Hungary / 29–31 August, 2012

bms.iit.bme.hu

Important dates

Submission of proposals
for invited speakers or sessions:
21 October, 2011
Paper submission deadline:
3 February, 2012
Notification of acceptance:
21 April, 2012
Final version due:
8 June, 2012

International Programme Committee

Balázs Benyó, IPC chair
Péter Várady, IPC vice-chair from industry
Steen Andreassen, IPC co-chair
David Feng, IPC co-chair
Ewart Carson, IPC co-chair
J. Geoffrey Chase, IPC co-chair
Levente Kovács, editor

Program Committee Members

Zoltán Benyó (HU)
Ruth Bars (HU)
József Bokor (HU)
Knud Buus Pedersen (DK)
Tom W. Cai (AU)
C.W. Chan (HK)
Kewei Chen (US)
Claudio Cobelli (IT)
Neil D. Evans (UK)
Thomas Desaive (B)
Paul Docherty (NZ)
Dario Farina (DK)
Niels Frimodt-Moller (DK)
Eiko Furutani (JP)
Keith R. Godfrey (UK)
Kevin Guelton (FR)
Oliver Haas (UK)
Per Hagander (SE)
Chris Hann (NZ)
Robert F. Harrison (UK)
Martin Hexamer (DE)
Henry Sung-Cheng Huang (US)
Dan Stieper Karbing (DK)
Jiri Kofranek (CZ)
György Kozmann (HU)
Gernot Kronreif (AT)
Kai Kueck (DE)
Adriaan Lammertsma (NL)
Aaron Le Compte (NZ)
Steffen Leonhardt (DE)
William S. Levine (US)
Claus Lindholt (DK)
Nigel Lovell (AU)
Stanislav Matousek (CZ)
Mahdi Mahfouf (UK)
Noureddine Manamanni (FR)
Johnny Ottesen (DK)
Béla Paláncz (HU)
Stephen Patek (US)
Bent Pedersen (DK)
Ulrike Pielmeier (DK)
Stephen Rees (DK)
Geoff Rodgers (NZ)
Su Ruan (FR)
Niilo Saranummi (FI)
Geoff Shaw (NZ)
Olaf Simanski (DE)
Michel Sorine (FR)
Vasile Stoicu-Tivadar (RO)
Josep Vehi (ES)
Xiuying Wang (AU)
Lingfeng Wen (AU)
Dwayne Westenskow (US)
Didier Wolf (FR)
Koon-Pong Wong (US)
Alina Zalounina (DK)
Janan Zaytoon (FR)
Tiange Zhuang (PRC)

Scope of the Symposium

The Symposium provide a forum for the presentation of new developments in the important interdisciplinary field of biomedical systems involving the application of concepts, methods and techniques of modelling, informatics and control of complex biomedical systems. The Symposium address problems in biomedicine, physiology and biology related to:

- model formulation,
- experiment design,
- identification and validation,
- biosignals analysis and interpretation,
- developments in measurement,
- signal processing,
- tracer kinetic modeling using various imaging systems,
- biomedical system modeling, simulation and visualization,
- decision support and control.

Application areas will include:

- celluar, metabolic, cardiovascular, neurosystems,
- healthcare management, disease control, critical care,
- pharmacokinetics and drug delivery,
- decision support systems for the control of physiological and clinical variables,
- biomedical imaging systems,
- intensive and chronic therapy,
- control of voluntary movements, respiration,
- rehabilitation engineering and healthcare delivery,
- kinetic modelling and control of biological systems and artificial organs,
- quantification of physiological parameters for diagnosis assessment.

Any other contributions to the development of modelling and control in biomedical and biological systems will be welcomed.

Registration Fee	Early	After 18.05.2012
Regular Registration Fee *	€ 450	€ 500
Student Registration Fee*	€ 300	€ 300
Extra paper fee	€ 60	€ 60
Banquet	€ 60	€ 60

* incl. all sessions, proceedings, three lunches, coffe breaks, banquet

Paper submission / Invited sessions and speakers

Papers must be submitted in PDF format according to the IFAC requirements. Accepted papers will be distributed at the symposium as pre-prints, and then published in electronic form on the IFAC-PapersOnLine web site (www.IFAC-PapersOnLine.net). Selected articles will be published in special issues of IFAC or IFAC-affiliated journals.
Suggestions for invited sessions and speakers/papers are welcome and can be submitted via the PaperCept site www.ifac.papercept.net/conferences/scripts/start.pl.

Social programs

Welcome reception–Banquet on the Danube–Lunches–Optional post-symposium tour

bms.iit.bme.hu

Indexing information

Infocommunications Journal is covered by INSPEC and Compendex.

The journal is supported by NCA NEMZETI CIVIL ALAPPROGRAM the National Civil Fund.

Infocommunications Journal

Technically co-sponsored by IEEE Hungary Section

Editorial Office (Subscription and Advertisements)**:**
Scientific Association for Infocommunications
H-1055 Budapest, Kossuth Lajos tér 6-8, Room: 422
Mail Address: 1372 Budapest Pf. 451. Hungary
Phone: +36 1 353 1027, Fax: +36 1 353 0451
E-mail: info@hte.hu
Web: www.hte.hu

Articles can be sent also to the following address:
Budapest University of Technology and Economics
Department of Telecommunications
Tel.: +36 1 463 3261, Fax: +36 1 463 3263
E-mail: szabo@hit.bme.hu

Subscription rates for foreign subscribers:
4 issues 50 USD, single copies 15 USD + postage

Publisher: PÉTER NAGY • Manager: ANDRÁS DANKÓ

HU ISSN 2061-2079 • Layout: MATT DTP Bt. • Printed by: FOM Media

www.infocommunications.hu

Network Optimization Techniques for Improving Fast IP-level Resilience with Loop-Free Alternates

Levente Csikor, Máté Nagy, Gábor Rétvári

Abstract—**Recently, due to the growing need for multimedia communication over IP, IP Fast ReRoute, the IETF standard for fast IP-level failure protection, has become very important. The basic specification for IPFRR is Loop-Free Alternates (LFA). LFA is simple and unobtrusive but, unfortunately, it usually does not provide full protection for all possible failure cases. Hence, many IPFRR proposals have come into existence, providing 100% failure coverage at the cost of significant changes and additional complexity to the IP infrastructure. Not surprisingly, therefore, currently LFA is the only IPFRR solution available in commercial routers. In consequence, there is now a growing need for network optimization techniques for improving LFA coverage in operational networks. In this paper, we present three such techniques. First, we investigate how to augment a network with only a few new links so as to maximize the number of protected failure scenarios. Then, we ask how the same effect can be achieved by optimizing the link costs. Finally, for the first time in the literature we combine the two aforementioned techniques into a single LFA network optimization framework. We show that these problems are all NP-complete and we give exact and approximate algorithms to solve them. Our numerical evaluations show that the combined algorithm is by far the most efficient for LFA network optimization and our methods can bring many networks close to perfect LFA coverage with only minor change in the topology.**

Index terms: IP protection, IP Fast ReRoute, Loop Free Alternates, Graph theoretical analysis, network optimization, combined metrics

I. INTRODUCTION

Recently, need for multimedia communication over IP, e.g., VoIP, streaming media, online gaming, video conferencing, and IPTV, has been increasing in an ever faster pace. For the Internet to become a truly ubiquitous platform for delivering dependable multimedia experience, however, IP communication services must guarantee the high reliability and five-nines availability (99.999% uptime) we got used to expect from the PSTN (Public Switched Telephone Network). Although the interruption of connectivity is tolerable for some traditional IP services, like WWW or email, it is devastating for real-time applications.

In an operational network, failures occur frequently due to various reasons, such as the disruption of a link, a router crash, a faulty interface, etc. One of the main design objectives of the Internet has been the ability to recover from failures seamlessly [1]. Consequently, standard intra-domain routing protocols, like OSPF (Open Shortest Path First) [2] and IS-IS (Intermediate System To Intermediate System) [3], were from the outset designed with tolerance for failures in mind. After a failure, adjacent nodes recognize it and distribute this information to every node in the network, which in turn recalculate shortest paths with the failed component removed from the topology. This re-convergence, however, assumes full flooding of new link states, which is a time consuming process (it can take between 150ms and a couple of seconds depending on network size and routers' shortest path calculation capabilities). During this period packets are dropped due to invalid routes. Several studies analyzed the common failure patterns in operational networks and their effect on the convergence of intra-domain routing [4]-[6]. Most recently, Markopoulou et al. showed that more than 85% of unplanned failures affect only links, and 46% of these failures are transient [7]. Unfortunately, such transient failures are very difficult to handle with current intra-domain routing protocols effectively, as just a single flapping interface is enough to keep all routers in the domain busy, constantly flooding the network with link state signaling traffic and recomputing shortest paths [7].

To answer this challenge, the IETF (Internet Engineering Task Force) defined the IP Fast ReRoute Framework (IPFRR, [8]) for native IP-level protection. The main goal is to reduce failure reaction time to tens of milliseconds and improve the handling of transient failures. IPFRR techniques are based on two major principles: *local rerouting* after a failure and sending packets on a *precomputed detour* avoiding global re-convergence. Locality means that only nodes adjacent to a failure know about it and they do not inform others. Precomputed, on the other hand, implies that the protection mechanism is proactive, so detours are computed and installed long before any failure occurs. Thus, if a link or node fails, adjacent nodes are able to switch to an alternate path, this way bypassing the failed component and enabling the intra-domain routing protocol to converge in the background. Note that bypassing a failure can lead to congestion and packet loss in parts of a network [5].

In the past few years, many IPFRR proposals have appeared but only one solution made it into commercial IP routers [9], [10]. This method is called Loop-Free Alternates. In LFA, when connectivity to a next-hop is lost all the traffic is re-routed to an alternate next-hop, called a Loop-Free Alternate, that still has a path to the destination that is unaffected by the failure. The alternate next-hop is selected in a way as to guarantee that it does not pass the packet back, because that would lead to an IPFRR loop and, eventually, to grave congestion and packet loss. Availability of a suitable LFA, however, strongly depends on the actual topology and the link costs. Thus, in most network topologies not all next-hops can be protected with LFA, leaving the network vulnerable to certain failure scenarios. Nevertheless, only this method was able to make its way to commercial routers, so instead of addressing any modifications to existing IPFRR methods or proposing new ones, we rather dealt with topological possibilities to improve LFA coverage.

Levente Csikor is with the *Budapest University of Technology and Economics, Department of Telecommunication and Media Informatics, High Speed Networks Laboratory* (e-mail: csikor@tmit.bme.hu).

Máté Nagy is with the *Budapest University of Technology and Economics, Department of Telecommunication and Media Informatics, High Speed Networks Laboratory* (e-mail: mate.nagy@tmit.bme.hu).

Gábor Rétvári is with the *Budapest University of Technology and Economics, Department of Telecommunication and Media Informatics, High Speed Networks Laboratory* (e-mail: retvari@tmit.bme.hu).

In this paper, network optimization techniques are presented in an attempt to manipulate the topology and link costs to improve the level of protection attainable with LFA. In particular, we propose three methods that promise significant improvement in LFA coverage: the *LFA graph extension* problem is concerned with augmenting a network with as few links as possible to maximize the number of LFA-protected failure cases; the *LFA cost optimization* problem asks for setting link costs for achieving the same objective; and the *combined LFA network optimization* problem asks for both adding new links *and* optimizing link costs to the same end. For each problem, we analyze the computational complexity, we propose approximate algorithms, and we provide extensive numerical experiments demonstrating the viability of our approach.

The rest of the paper is organized as follows. In Section II, related works are discussed. Section III is devoted to introduce the model and notations for our LFA network optimization framework and providing some simple graph-theoretical bounds on LFA coverage. The LFA graph extension problem is discussed in Section IV, the LFA cost optimization problem is studied in Section V, and the combined LFA network optimization problem is considered in Section VI. Finally, we conclude our work in Section VII.

II. Related work

The Loop-Free Alternates method can usually protect only about 50-80% of the possible link failure scenarios, and the level of node protection is even worse [11-14]. Consequently, since LFA appeared many other proposals have surfaced to overcome the limitations inherent to it.

In [11] the authors presented a detailed measurement study of all the factors that on a router influence the convergence time attainable by an intra-domain routing protocol. This is characterized by "detection time + link state information origination time + distribution delay + flooding time + shortest path tree computation + update of routing table". They showed that a couple of hundreds of milliseconds can be achieved with IS-IS in case of link failures. Even though this study demonstrates that sub-second convergence can be provided even with current router technology, unfortunately this is still too large for applications with real-time demands.

The main idea of *Failure-carrying Packets* (FCP [15]) is as follows. A simple backup mechanism can only deal with the failure of single node/link. However, in order to provide guarantees for simultaneous failures of multiple arbitrary nodes/links, the number if precomputed paths needed is extremely high. In FCP, all routers have a consistent view of potential links (i. e. those that are supposed to be operational) called a Network Map. Because of its consistency, all that needs to be carried by packets is information about which of these links have failed. The authors also proposed a variant called Source-Routing FCP providing similar properties even if the network maps are inconsistent.

In *O2 (outdegree 2) routing* [16], each router holds multiple alternate paths through at least two distinct next-hops to each destination, in order to facilitate local failure reaction and loop-free destination based routing. By using two next hops, a node detecting an adjacent failure can re-distribute packets to the remaining next-hop instantly. Consequently, the network must meet a necessary condition: each node must form at least one triangle with its neighbors. The authors show that this necessitates using "joker" links, serving only for protecting certain failure cases instead of actively participating in default packet forwarding.

Another approach is using a small set of backup network configurations, called *Multiple Routing Configurations* (MRC, [17]). For each configuration, the standard routing algorithm calculates configuration specific shortest paths. Thus, for any single link or node failure a nearby router detects it and marks the packet with a backup configuration identifier designating an overlay topology that does not contain the failed component. Studies proved that the number of backup configurations needed is usually only three or four.

A qualitative protectability analysis for a fast resilience scheme called *protection routing* is presented in [18]. Protection routing is based on centralized control over the routing tables [18]. In general, centralized control brings numerous disadvantages, above all scalability and latency in reacting to failures. The latter arises from having to notify a central server and communicate the updated forwarding information back to all affected routers before the network can react to a failure. Protection routing solves this problem through a preventive mechanism, in which a central server pre-computes forwarding decisions for common failure scenarios and downloads these in the routers. Thus, after a failure the appropriate new forwarding state is already available locally. Thanks to the use of a central server, forwarding paths and detours do not necessarily depend on a common set of link weights, leaving broader range for improving the level of protection.

In the IPFRR method called *Not-via addresses* [19], when a failure occurs packets affected by it are encapsulated in a new IP header with an address that explicitly identifies the network component that the detour must avoid. In other words, Not-via uses the destination address in IP packets to mark whether the packet is being forwarded on the default path or in a tunnel along a detour. Unfortunately, at the moment there is no standardized protocol for advertising not-via addresses. Moreover, Not-via brings additional complexity into routing and, if the additional IP header does not fit into the MTU, it can cause packet fragmentation and time-consuming re-assembly at the tunnel endpoint. The *lightweight version of Not-via* [20] was proposed to bring down the management and computational complexity of Not-via. Lightweight Not-via is based on the concept of redundant trees [21]. Redundant trees are basically a pair of directed spanning trees having the appealing property that a single node or link failure destroys connectivity through only one of the trees, leaving the path along the other tree intact. This technique can significantly decrease the number of Not-via address (to a constant 3 addresses per node) and eliminates most of Not-via's computational complexity.

Another family of IPFRR techniques, called *Failure Insensitive Routing*, uses interface specific forwarding (FIR [22], FIFR [23]). FIR handles only link failures while FIFR takes care for node failures as well. If a node receives a packet through an unusual interface, it can infer implicitly the cause of the failure and a next-hop is chosen that bypasses the failed component. Unfortunately, interface specific forwarding is generally not available in IP routers today. In a nutshell, many proposals for IPFRR have appeared but all of them need

significant modifications to current routing protocols or changing IP's destination based forwarding (as in FIR); introduce some forms of signaling to indicate that a packet is on a detour; require extra bits in the IP header (like in MRC); or use tunnels imposing additional address management burden on the operator (like Not-via). Loop-Free Alternates, however, does not require any of these. Hence, it is straightforward to implement LFA in routers and deploy it in operational networks. As such, in our days LFA is the only IPFRR method available in off-the-shelf routers, despite of the fact that it usually cannot provide 100% failure protection in all networks. There is, therefore, an increasing demand for LFA-oriented network optimization methods that can improve the quality of protection provided by LFA in operational networks.

III. Loop-Free Alternates: Analysis

Throughout this paper, a network topology is modeled as a *simple, undirected, weighted graph* $G(V, E)$ with V being the set of nodes and E the set of edges. Let $n = |V|$ and $m = |E|$, and denote an edge as *(i, j)*, where i and j are nodes from V. Link costs are represented by a cost function $c : E \Rightarrow \mathbb{N}$. The cost of a link *(i, j)* is denoted with *c(i, j)*.

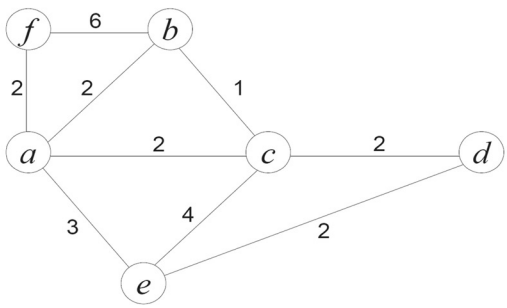


Figure 1. A simple weighted network topology

Perhaps the easiest way to understand how LFA works is through an example. Consider the network depicted in Figure 1 and suppose that node *a* wants to send a packet to the destination denoted by *d*. The next-hop of *a* along the shortest path towards *d* is *c*.

If link *(a, c)* fails, then *a* has to find an alternative neighbor to pass on the packets destined to *d*. It cannot send these packets to, say, *f*, as *f* 's shortest path to *d* goes through itself, so *f* would send the packet back causing a loop. This is because, as mentioned above, in IPFRR only adjacent routers are aware of a failure, so in this case *f* does not know that link *(a,c)* has disappeared and so it blindly uses its shortest path through the failed link. Instead, *a* needs to find a neighbor which is closer to the destination than the route from the neighbor through itself. Such neighbors are called Loop-Free Alternates (LFAs). In general, for some source node *s* and destination *d*, a neighbor *n* of *s* that is not the default-next-hop is a *link-protecting LFA* if

$$dist(n,d) < dist(n,s) + dist(s,d) \ , \qquad (1)$$

where *dist(x,y)* denotes the length of the shortest path between *x* and *y*. (Note that, for the sake of simplicity, herein we disregard for Equal-Cost MultiPath and we shall concentrate on the link-protecting case exclusively. The development goes similarly when these assumptions do not hold, but the notation is significantly more complex [28].) For example, if link *(a, c)* fails then node *e* is a link-protecting LFA, because its shortest path to destination *d* avoids the failed component. For this source-destination pair, *e* is a *node-protecting LFA* for the failure of node *c*, because its shortest path doesn't go through *c*. Node *e* is also a *per-link LFA* for the link *(a, c)* as it protects all the nodes reachable by *a* through *(a, c)*. Now, consider node *d* as source and node *c* as destination. If link *(d, c)* fails, the only alternate neighbor, node *e,* is not an LFA, because it does not fulfill (1). Hence, this particular failure case cannot be protected by LFA.

To measure LFA failure coverage in a network G over the cost function *c*, we use the simple metric adopted from [24]:

$$\eta(G,c) = \frac{\#\, LFA\ protected(s,d)\ pairs}{\#\, all(s,d)\ pairs}$$

One easily sees that $\eta(G,c)=1$ if and only if each node has an LFA towards each other node, and in general $\eta(G,c)$ varies between 0 and 1 depending on the actual network topology and link costs. We tightened this general characterization in [25] as follows.

Theorem 1: The failure coverage of a 2-connected graph G on n nodes is bounded by $\frac{1}{n-1} \le \eta(G,c) \le 1$, and the lower bound is tight for rings with even number of nodes and uniform costs.

This observation has two important implications. First, there is no network with exactly zero LFA coverage, but as n grows the proportion of LFA-protected failure cases to all failure cases can approach zero arbitrarily close. Second, the Theorem implies that it is the even ring topology that has the smallest LFA coverage out of all 2-connected graphs with the same number of nodes. This is not surprising in light of the fact that rings have been shown to be detrimental to other IPFRR mechanisms as well earlier [26],[27]. For complete proof, see [25]. In [28], we sharpened these bounds as follows:

Theorem 2: For any connected simple graph G with $n > 2$ and any cost function c:

$$\frac{n}{n-1}\,\frac{\Delta/2-1}{\Delta_{max}-1} + \frac{1}{n-1}(\Delta_{max}-1) \le \eta(G,c) \le \frac{n}{n-1}(\Delta-2) + \frac{2}{n-1} \ ,$$

where Δ is the average node-degree in G and Δ_{max} is the maximum node-degree.

IV. LFA Graph Extension

In this section, we show how to increase the level of LFA protection by cleverly adding new links to the network. For instance, if one added the edge *(d,b)* of cost, say, 10, to the sample topology in Figure 1, then the so far unprotected source-destination pair *(d,c)* would gain an LFA. Motivation for increasing the LFA coverage this way is the recognition that in many cases augmenting the topology with new links, however costly, is still preferred over changing the link costs. This is because very often an operator pays special attention to properly engineer the link costs according to his or her own specific operational objectives, like minimizing delay, balancing load to eliminate congestion, etc., and optimizing

link costs just for LFA would interfere with these operational goals. In these cases, installing new links or leasing additional capacity is an effective way to improve LFA coverage. In order to guarantee that the cautiously engineered shortest paths remain intact, we set the cost of the added links sufficiently high, typically, to a value greater than the length of the longest shortest path. Obviously, we want to install the minimum number of auxiliary links to minimize expenditures and eventually we want to attain full LFA coverage. This problem is called the *LFA graph extension* problem, and it is formally defined as follows [25]:

Definition 1: Given a simple, undirected, weighted graph *G(V, E) and an integer k*, is there a set $F \subseteq \overline{E}$ with $|F| \leq k$ and properly chosen cost function c, so that $\eta(G(V, E \cup F), c) = 1$ and the shortest paths in *G(V, E)* coincide with those in $G(V, E \cup F)$?

Note that $\overline{E}$ denotes the complement of the edge set *E*. The above definition is deliberately formulated as a decision problem, so that it readily lends itself to the following complexity characterization.

Theorem 3: The LFA graph extension problem is NP-complete.

For a complete proof, see [25]. Usually, instead of the decision form, we want to solve the optimization version where we ask for adding the smallest number of new links to attain complete LFA coverage. Easily, this optimization version is also intractable by Theorem 3. To solve it, an optimal Integral Linear Program (ILP) is proposed in [25]. For large networks, however, the ILP might be impossible to solve to optimality. This raises the demand for efficient and computationally tractable heuristics, which promise a good approximation for the solution of the LFA graph extension proposition. Below, we trace back this question to the *Minimum set cover problem* problem, a well-known NP-compete problem, and we collect some heuristic algorithms from the literature to obtain an approximate solution to it.

Before turning to the algorithms, we note that in certain cases LFA coverage can not be improved to 100% just by adding complementary edges to the network. In [25], a polynomial time preprocessing method is presented that modifies the topology, making the problem solvable. Below, we silently assume that this preprocessing phase has already been applied to the input graph.

A. Model

First, we show that any instance of the LFA graph extension problem can be converted to an equivalent instance of the minimum set cover problem in polynomial time.

Consider the example topology in Figure 2. This graph does not have full link-protecting LFA coverage, as node *e,* for instance, does not have an LFA towards *a*. Let us examine what happens if new links are installed. Not all the complementary edges provide additional protection, e. g., establishing a new link between *a* and *d* would not increase the LFA coverage in the graph. In particular, a new link creates LFA for a well-defined subset of the unprotected node pairs, and this subset is easy to compute. Then, the idea is that if we match the set of unprotected source-destination pairs with the complementary edges that provide LFA to them, then we obtain a bipartite graph, and solving the LFA graph extension problem on the original graph is equivalent to solving the minimum set cover problem on the bipartite graph representation.

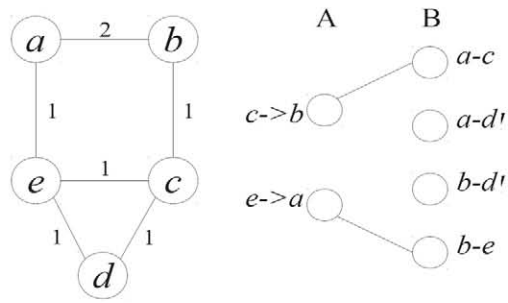


Figure 2: Bipartite graph model for LFA coverage improvement

Let $(s,d)_i : i \in 1,2,...,k$ be the set of source-destination node pairs that have no LFA protection and let $e_j : j \in 1,2,...,l$ be the set of complementary edges in *G(V, E)*. Let $G'(A, B, F)$ be a bipartite graph with node set $A \cup B$ and edge set *F*. Here, we add a node $a_i \in A$ corresponding to each $(s,d)_i$ pair and a node $b_j \in B$ to each e_j complementary edge. Connect some $a_i \in A$ to some $b_j \in B$ in G' if and only if e_j , when added to *G* with suitably large cost, would provide a link-protecting LFA to $(s,d)_i$. Then, it is easy to see that the LFA graph extension problem in *G* is equivalent to the minimum set cover problem in the corresponding $G'(A, B, F)$ bipartite graph formulated as follows: find the minimum set of nodes *C* in *B* (a cover), so that every node in *A* has at least one neighbor in *C*. Note that this is still NP-complete, however, there are plenty of well-tested heuristics available in the literature to approximate it. For the purposes of this paper, we chose four efficient heuristics, namely, the Lovász-Johnson-Chvatal (LJC) algorithm from [31], and the SBT, RSBT and MSBT algorithms from [30]. Note that these heuristics are in fact formulated for the *Minimum hypergraph transversal* problem, but this is equivalent to minimum set cover.

B. Approximate algorithms

Next, we go briefly through each of the selected heuristics. For more details and pseudo-codes, consult [29].

1. The Lovász-Johnson-Chvatal method (LJC): In every iteration the edge is inserted which improves LFA coverage the most. In particular, in every step the highest degree node $v \in B$ is chosen and added to the cover while all its neighbors from *A* are deleted. Unfortunately, the method does not always find a cover that is *minimal in the sense of inclusion*, which practically means that some subset of the resultant cover could also be an adequate cover.

2. SBT: Unlike LJC, the SBT algorithm always finds the set that is minimal in the sense of inclusion. In every iteration, it looks for the node $v \in B$ with the smallest degree and removes it from *B*. If any neighbor of *v* exists in *A* that was only covered by this *v*, then *v* is added to the cover. In this case all its neighbors are considered as covered and we remove them from *A,* and we go on with the next iteration.

3. RSBT: This algorithm works as the reverse of SBT, as in every step it seeks for the node $v \in B$ with the highest degree instead of the smallest degree. All other steps are the same.

4. MSBT: MSBT is a slightly modified version of SBT. Similarly to SBT, in the first phase it looks for a node $v \in B$ with the smallest degree and if there are nodes in A covered only by v, then v will be added to the cover. If the latter condition is not satisfied, then all the neighbors *neigh(v) of v* in A are checked, if there exists a node covered exactly by one node from B other than v. In other words, the algorithm looks for nodes $w \in neigh(v)$ with degree two. We add the nodes connected to these ws from B to the cover, and we remove them from B and all their neighbors from A. Then, we proceed to the next iteration.

Suppose that a heuristic algorithm has terminated with the cover $C \subseteq B$. Then, we obtain an approximation of the original LFA graph extension problem by adding the new links $e_j : b_j \in C$ to the network with sufficiently large cost.

C. Numerical Evaluation

We conducted extensive numerical evaluations with the heuristics on several real-world service provider topologies. The Abilene, Italy, Germany, NSF, AT&T, and the extended German backbone networks are taken from [32] and [33]. All other networks were used from [34]. Wherever available, we used the original link costs that came with the networks. In other cases, costs were set uniformly to one unit. The results are presented in Table 1 with the following notations: n represents the number of nodes and m the number of links in the network; $\eta(G, c)$ is the initial LFA coverage; the column ILP shows the optimal solution for the LFA graph extension obtained by the ILP in [25] (i.e., the minimum number of new links needed to attain full LFA coverage), and the LJC, SBT, RSBT and MSBT columns give the number of links as produced by the respective approximation method. We found that among the heuristics the MSBT algorithm offers the fewest links in general, with LJC as close second. In most cases, the approximation misses the optimum with only a few links. There are some exceptional cases, however, especially large networks, where the difference is more significant. Additionally, the results clearly state that the solution to the LFA graph extension problem is highly topology dependent: for smaller networks usually only a handful of new links is enough, while large networks can require dozens of links to achieve full protection. For such cases, it might be more beneficial to aim for merely increasing LFA coverage into a given safe range, say, above 90%, instead of shooting for complete protection. To see how our heuristics fit for this objective, we took a deeper look at the coverage during the processing of each heuristic in order to assess how LFA coverage improves with each new link added. The results for the Italian backbone are given in Figure 3. We observe that in the first steps it is the LJC algorithm that improves LFA coverage the most. In our case, LFA coverage is increased to 90% with only 3-4 new links, and it rapidly reaches more than 98%. Our conclusion is that solving the LFA graph extension problem requires fundamentally different approximation strategies depending on the actual optimization objective: if full coverage is the aim then the MSBT algorithm is the best choice, while it is the LJC algorithm that ensures the fastest increase in the LFA coverage initially.

1. TABLE: EXACT AND APPROXIMATE SOLUTIONS FOR THE LFA GRAPH EXTENSION PROBLEM IN REAL TOPOLOGIES.

Name	n	m	η(G,c)	ILP	LJC	SBT	RSBT	MSBT
AS1221	7	9	0.809	2	2	2	2	2
AS1239	30	69	0.873	6	6	7	11	6
AS1755	18	33	0.872	7	7	9	12	7
AS3257	27	64	0.923	10	11	10	12	10
AS3967	21	36	0.785	8	11	10	16	9
AS6461	17	37	0.933	3	3	3	4	3
Abilene	12	15	0.56	7	8	9	14	8
Italy	33	56	0.784	17	22	28	39	19
Germany	17	25	0.695	9	12	12	13	11
NSF	26	43	0.86	11	12	13	28	13
AT&T	22	38	0.822	10	12	12	12	11
Germ_50	50	88	0.9	18	21	29	44	25
Arnes	41	57	0.623	24	29	24	30	24
Deltacom	113	161	0.577	80	100	94	131	91
Geant	37	55	0.69	21	23	21	25	21
InternetMCI	19	33	0.904	5	6	5	5	5
Average:	**30.6**	**51.2**	**0.79**	**14.87**	**17.81**	**18**	**24.87**	**16.56**

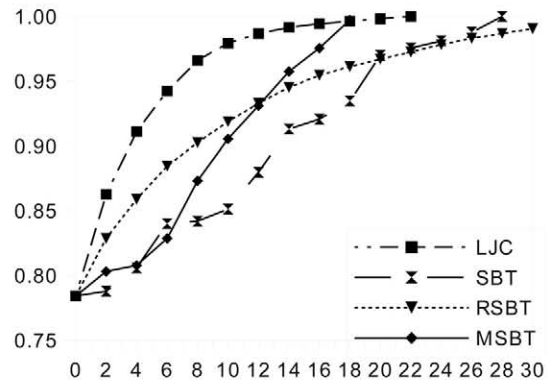


Figure 3. LFA coverage tendency in Italy networks

V. LFA COST OPTIMIZATION

In some networks, adding new physical links to the topology is very difficult or costly, therefore, LFA graph extension cannot be applied for improving failure case coverage. In such cases, it may be worth reconfiguring the link costs, even if this may alter the shortest paths that have been engineered to match the operational goals of the operator previously, because the gain in availability can easily compensate for the loss in forwarding efficiency. As shall be shown in numerical evaluations soon, optimizing costs for LFA can result in high improvements in failure case coverage, to the point that in many network topologies even close to perfect LFA coverage can be reached. The *LFA cost optimization* problem asks for a link cost setting that maximizes the LFA coverage, given inherent limitations of the network topology under consideration. It is formulated as follows:

Definition 2: Given a graph G, is there a cost function c so that $\eta(G, c)=1$?

Again, the LFA cost optimization is formulated above as a decision problem in order to be later subjected to complexity analysis. In practice, however, we are much more interested in the optimization version, which asks for the cost setting that maximizes the LFA coverage. In [28], we proved the following result.

Theorem 4: The LFA cost optimization problem is NP-complete.

Surprisingly, we found that even the task of assigning LFAs to *just a single* destination is already NP-complete. This suggests that this problem is very difficult to solve. And indeed, the ILP we gave in [28] is only applicable in very small networks (up to approx. less than 10 nodes), and thus for larger networks, we need to resort to heuristics.

A. Approximate Algorithms

Below, we present a Simulated annealing-based heuristic, which promises a high quality approximation of the optimal solution in polynomial time [28].

Algorithm 1. Heuristic LFA cost optimization algorithm. Input is graph G.

1: $c \leftarrow$ random_cost(C_{max}), $T \leftarrow T_0$
2: **while** $T > 0$ and $\eta(G, c) < 1$
3: $c' \leftarrow$ argmax $\eta(G, q)$, where $q \in$ neigh(c)
4: **if** $\eta(G, c') > \eta(G, c)$ or $T >$ random(T_0) **then**
5: $c \leftarrow c'$
6: **end if**
7: $T \leftarrow T - 1$
8: **end while**

Our heuristic LFA cost optimization algorithm given in Alg. 1 works as follows. Given the network as input, first the costs are randomized (random_cost function) between 1 and C_{max} (where C_{max} is a problem parameter, chosen as C_{max}=20 below) and the initial temperature T is set to T_0 (again a parameter, set to 150 in our numerical studies). While the temperature T is greater than 0 and $\eta(G,c)$ is less than 1, we perform the following iteration: take the actual cost function and increase or decrease (if possible) the cost by one at exactly one link. Line 3 searches for the best such neighbor. Do this for all links, and choose the cost function that produces the highest LFA coverage. If the new cost vector is better than the present phase (in terms of η), it is unconditionally accepted. Otherwise, accept it only if a random number generated between 0 and T_0 is less than the actual temperature T as described in Line 4. Decrease T and proceed to the next iteration. This way, the algorithm easily escapes from local minima at the initial steps, to eventually settle in a good local minimum by only letting greedy steps when T is low. We also apply a tabu list of size 20 to preclude the algorithm from oscillating. In order to let the algorithm discover the largest range of the problem space possible, we execute N rounds (where in our evaluations N=500) and we choose the cost function c^* that yields the highest LFA coverage in all rounds.

B. Numerical Evaluation

We conducted thorough numerical studies in order to assess the extent to which LFA coverage can be improved by optimizing link costs. The numerical evaluations were run on the same networks as presented in the previous section. Table 2. shows the results, in order of appearance: characteristics of the topologies (name, number of nodes n, number of edges m), LFA coverage $\eta(G, c)$ obtained by the original cost setting c, and the LFA coverage $\eta(G, c^*)$ for the best cost function c^* obtained by the heuristic algorithm presented previously.

2. TABLE: APPROXIMATE SOLUTIONS TO THE LFA COST OPTIMIZATION PROBLEM IN REAL TOPOLOGIES

Name	n	m	η(G, c)	η(G, c*)
AS1221	7	9	0.809	0.833
AS1239	30	69	0.873	0.957
AS1755	18	33	0.872	0.98
AS3257	27	64	0.923	0.997
AS3967	21	36	0.785	0.967
AS6461	17	37	0.933	0.996
Abilene	12	15	0.56	0.701
Italy	33	56	0.784	0.919
Germany	17	25	0.695	0.889
NSF	26	43	0.86	0.95
AT&T	22	38	0.822	0.984
Germ_50	50	88	0.9	0.934
Arnes	41	57	0.623	0.702
Deltacom	113	161	0.577	0.662
Geant	37	55	0.69	0.74
InternetMCI	19	33	0.904	9.932

The most important observation is that in many real network topologies close to perfect LFA coverage can be achieved with cost optimization. Nevertheless, there were some exceptional topologies where LFA cost optimization was less appealing. Our results indicate that LFA cost optimization greatly helps the operator to provide higher availability in the network, even when adding new connectivity to the topology is not feasible. In addition, we found that the running time of the approximation algorithm strongly depends of the topology, in particular, on the number of links and nodes. In some cases, all 500 rounds terminate in just a couple of minutes, but sometimes it takes a couple of hours. Note that running time is not that important in practice, because LFA cost optimization is performed offline only once, before the final deployment of a network.

VI. COMBINED LFA NETWORK OPTIMIZATION

So far, we have shown that both adding new links to a network and optimizing link costs are effective ways of improving the LFA coverage in operational networks. It is of question, however, to what extent the combination of these two methods can be effective for LFA-based network optimization. Hence, in this section we propose the *combined LFA network optimization* problem as the combination of the aforementioned two methods. This problem is formulated as follows:

Defintion 3: Given a simple, undirected, weighted graph $G(V,E)$ and a positive integer k, is there a set $F \subseteq E$ with $|F| \leq k$ and properly chosen cost function c, so that $\eta(G(V,E \cup F),c)=1$?

The difference from the LFA graph extension problem is that in the above formulation we allow for link costs and, consequently, the shortest paths to change. Note that for k=0 we obtain the LFA cost optimization problem, which immediately implies the following result.

Theorem 5: The combined LFA network optimization problem is NP-complete.

Easily, again an optimization version can be defined which asks for the minimum number of new links and an appropriate cost function, which, when applied to the network, result complete LFA coverage.

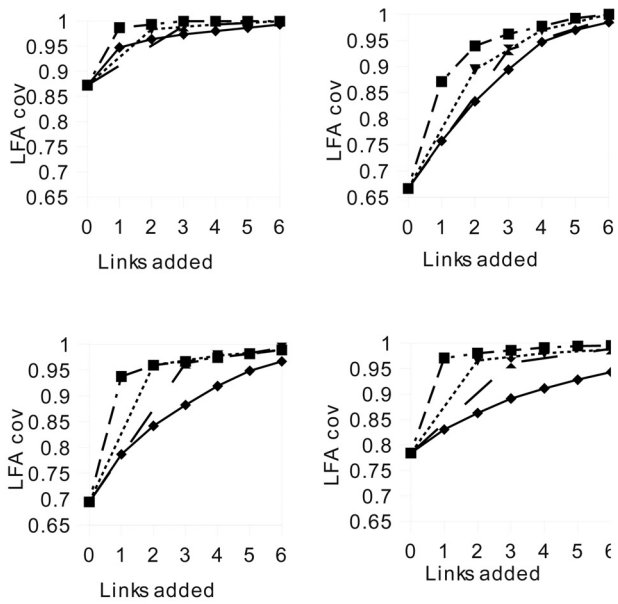
A. Approximate algorithm

From all the optimization problems treated so far, combined LFA network optimization is the most difficult. Therefore, instead of aiming for an optimal solution, in this paper we propose a heuristic algorithm based on the consecutive application of the heuristics presented for the individual subproblems in the previous sections. In particular, in every iteration we execute an LFA graph extension phase followed by an LFA cost optimization phase. In the LFA graph extension phase, we add l new links to the network (where l is a problem parameter) by using the LJC algorithm. This algorithm is chosen because it promises the largest increase in LFA coverage. In the LFA cost optimization phase, we compute a link cost setting that approximately maximizes the LFA coverage on the augmented graph obtained in he previous phase. The two phases are applied iteratively one after the other, until the LFA coverage reaches 1.

B. Numerical evaluations

In order to evaluate the performance of the combined algorithm as compared to the individual algorithms, we conducted several rounds of numerical experiments. Herein, we present the results for only a subset of the network topologies introduced in the previous sections. Similar results were obtained for the rest of the topologies.

First, we were curious as to what is the optimal setting for the parameter l. We experimented with the settings $l \in [1,2,3]$, as during our numerical studies we found that at most 3 new links is always enough to realize a reasonable improvement in LFA coverage. The results can be seen in Figure 4. For each network topology, the simple dashed line represents the LFA coverage realized by LFA graph extension alone (i.e., with no LFA cost optimization phase applied) as of the LJC algorithm, and the dotted dashed line, the fine-dotted line and the solid line give the LFA coverage for the combined algorithm for the case $l=1$, $l=2$, and $l=3$, respectively. Easily, for the case when $l=1$ we have a data point for each iteration, but for other cases some of these internal data points are missing, as improvement only appears after adding more than one link in such cases. The results show that the combined algorithm performs best when in every LFA graph extension phase we add only a single link, and this is immediately followed by a cost optimization phase. In consequence, we used the setting $l=1$ in the rest of the study.



4. Figure: Results of the several combined metrics (AS1755, Abilene, Germany, Italy)

After fixing l, we turned to the main question of our numerical studies: to what extent the combined algorithm outperforms previous algorithms? The results for some selected topologies are given in Table 3, which shows in order of the appearance: the characteristics of the topologies (name, number of nodes n and edges m); the initial LFA coverage $\eta(G,c)$; LFA coverage achieved with simple LFA graph extension in step 1, 2, 3, 4, 5, 6, and the number of links needed for full coverage (denoted by hashmark); and finally the same results obtained by the combined LFA network optimization algorithm. For the combined algorithm, the LFA coverage values in bold highlight the cases when the LFA cost optimization phase did not improve LFA coverage at all. Our results suggest that the combined algorithm reaches complete coverage with much fewer links than the LFA graph extension algorithm (the difference is highlighted in Figure 5). This is

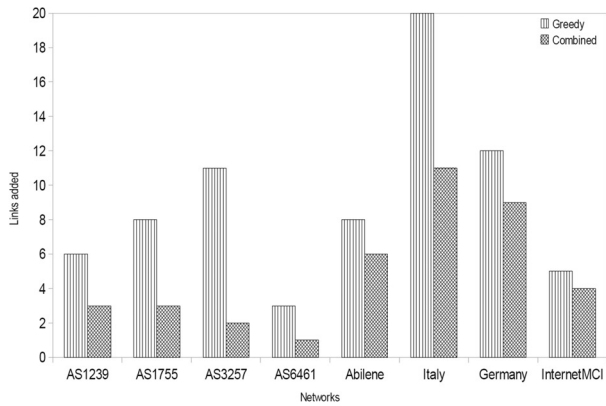


Figure 5.
Number of links needed to be added using the different algorithms

Topology				LFA Graph Extension							Combined LFA Optimization						
Name	**n**	**m**	**η(G,c)**	**1**	**2**	**3**	**4**	**5**	**6**	**#**	**1**	**2**	**3**	**4**	**5**	**6**	**#**
AS1239	30	69	0.873	0.932	0.971	0.985	0.992	0.997	1	**6**	0.994	0.998	1	-	-	-	**3**
AS1755	18	33	0.872	0.947	0.964	0.973	0.980	0.986	0.993	**8**	0.986	0.993	1	-	-	-	**3**
AS3257	27	64	0.923	0.971	0.983	0.987	0.990	0.991	0.993	**11**	0.998	1	-	-	-	-	**2**
AS6461	17	37	0.933	0.985	0.996	1	-	-	-	**3**	1	-	-	-	-	-	**1**
Abilene	12	15	0.56	0.757	0.833	0.894	0947	0.969	0.985	**8**	0.871	0.939	**0.962**	**0.977**	0.992	1	**6**
Italy	33	56	0.784	0.830	0.862	0.891	0.911	0.928	0.943	**20**	0.970	**0.980**	**0.985**	**0.991**	**0.994**	**0.995**	**11**
Germany	17	25	0.695	0.786	0.841	0.882	0.920	0.948	0.966	**12**	0.937	**0.959**	**0.966**	**0.974**	**0.981**	**0.988**	**9**
InternetMCI	19	33	0.904	0.973	0.985	0.994	0.997	1	-	**5**	0.991	**0.994**	**1**	-	-	-	**4**

TABLE 3. RESULTS FOR THE LFA GRAPH EXTENSION AND THE COMBINED LFA NETWORK OPTIMIZATION ALGORITHMS.

not surprising, as the combined algorithm is free to reconfigure link costs, which the LFA graph extension algorithm is not permitted to do.

We find that the combined algorithm significantly reduces (in average by more than 50%) the number of additional links necessary for reaching 100% LFA coverage. We also found that it is not worth running all the 500 rounds of the LFA cost optimization algorithm as we did previously, because in the combined algorithm the optimum was always realized in less than 200 rounds.

VII. CONCLUSIONS

In this paper, we proposed several network optimization algorithms for improving the level of fast IP-level resilience using Loop-Free Alternates, the only IPFRR technique available in commercial routers out-of-the-box today. First, we described the LFA graph extension problem, which asks for establishing new links to increase LFA coverage without altering the shortest paths in the network. Second, we presented an LFA cost optimization problem which, instead of adding new links, rather calls for modifying link costs to instantiate new LFAs. Finally, for the first time in the literature we presented a combined formulation. On the theoretical side, we found that each of the three network optimization problems are intractable. On the practical side, we proposed several approximation strategies for solving the problems on real instances and our numerical results suggest that each method is suitable to attain a 10-40% improvement in LFA coverage. We also found that the results strongly depend on the actual network topology. The combined algorithm was found to produce the best results, indicating that in many real networks complete LFA-based protection is attainable with adding only a few new links. We believe that the wide spectrum of LFA network optimization strategies presented in this paper provide a rich set of options for operators to choose from, according to their own preference on whether it is economically more feasible to add new links, change costs, or do both, to improve LFA-protection in their network.

Future works involves fine-tuning the parameters of the approximation algorithms, and a customization of the algorithm for the more realistic cases when, for instance, not all source-destination pairs need to be protected or some source-destination pairs have higher priority than others; only certain shortest paths must be retained but others can change arbitrarily; or the costs are optimized both for LFA coverage *and* to provide efficient utilization of the network with respect to the expected traffic matrix.

ACKNOWLEDGMENT

G.R. was supported by the János Bolyai Fellowship of the Hungarian Academy of Sciences. The project was supported by TÁMOP 4.2.2.B-10/1-2010-0009 grant.

REFERENCES

[1] D. D. Clark, „The design philosophy of the DARPA internet protocols," SIGCOMM, Computer Communications Review, vol. 18, no. 4, pp. 106-114, Aug. 1988.

[2] J. Moy, „OSPF Version 2," RFC 2328, Apr. 1998.

[3] ISO, „Intermediate System-to-Intermediate System (IS-IS) Routing Protocol," ISO/IEC 10589, 2002.

[4] C. Labovitz, G. R. Malan, F, Jahanian, „Internet Routing Instability," IEEE/ACM Transactions on Networking, vol. 6, no. 5, pp. 515-528, 1998.

[5] S. Iyer, S. Bhattacharyya, N. Taft, C. Diot, „An approach to alleviate link overload as observed on an IP backbone," in Proc. Infocom, 2003.

[6] ETSI Document EN 300416 V1.2.1, „Network Aspects (NA): Availability Performance of Path Elements of International Digital Paths," Aug. 1998.

[7] A. Markopoulou, G. Iannacone, S. Bhattacharyya, C-N. Chuah, C. Diot, „Characterization of Failures in an IP backbone," in Proc. IEEE Infocom, Mar. 2004.

[8] M. Shand, S. Bryant, „IP Fast Reroute Framework," RFC 5714, Jan. 2010

[9] „Cisco IOS XR Routing Configuration Guide, Release 3.7," Cisco Press, 2008.

[10] „JUNOS 9.6 Routing protocols configuration guide," Juniper Networks, 2009.

[11] P. Francois, O. Bonaventure, „An evaluation of IP-based fast reroute techniques," in ACM CoNEXT, 2005, pp. 244-245.

[12] S. Previdi, „IP Fast ReRoute technologies," APRICOT, 2006.

[13] M. Gojka, V. Ram, X. Yang, „Evaluation of IP fast reroute proposals," in IEEE Comsware, 2007.

[14] M. Menth, M. Hartmann, R. Martin, T. Čičić, A. Kvalbein, „Loop-free alternates and not-via addresses: A proper combination for IP fast reroute?" Comput. Netw., vol. 54, no. 8, pp. 1300-1315, 2010.

[15] K. Lakshminarayanan, M. Caesar, M. Rangan, T. Anderson, S. Shenker and I. Stoica, „Achieving convergence-free routing using failure-carrying packets," in. Proc. SIGCOMM, 2007.

[16] G. Schollmeier, J. Charzinski, A. Kirstädter, C. Reichert, K. Schrodi, Y. Glickman, C. Winkler, „Improving the resilience in IP Networks," in. Proc. HPSR, 2003.

[17] A. Kvalbeinm A. F. Hansen, T. Čičić, S. Gjessing, O. Lysne, „Fast IP network recovery using multiple routing configurations," in Proc. IEEE INFOCOM, 2006.

[18] K.-W. Kwong, L. Gao, R. Guerin, Z.-L. Zhang, „On the Feasibility and Efficacy of Protection Routing in IP Networks," in INFOCOM 2010, long version is available in Tech. Rep. 2009, University of Pennsylvania, 2010.

[19] S. Bryant, M. Shand, S. Previdi, „IP fast reroute using Not-via addresses," Internet Draft, available online: http://www.ietf.org/internet-drafts/draft-ietf-rtwg-ipfrr-notvia-addresses-00.txt, Feb. 2008.

[20] G. Enyedi, P. Szilágyi, G. Rétvári, and A. Császár, "IP Fast ReRoute: Lightweight Not-Via without Additional Addresses", in Proc. INFOCOM, pp.2771-2775, 2009.

[21] M. Médard, R. A. Barry, S. G. Finn, R. G. Galler, „Redundant trees for preplanned recovery in arbitrary vertex-redundant or edge-redundant graphs," IEEE/ACM Transactions on Networking, vol. 7, no.5, pp. 641-652, Oct. 1999.

[22] S. Lee, Y. Yu, S. Nelakuditi, Z.-L. Zhang, C.-N. Chuah, „Proactive vs. Reactive Approaches to Failure Resilient Routing", in Proc. IEEE INFOCOM, Hong Kong, 2004.

[23] Z. Zhong, S. Nelakuditi, Y. Yu, S. Lee, J. Wang, C.-N. Chuah, „Failure Inferencing based Fast Rerouting for Handling Transient Link and Node failures", in IEEE INFOCOM, 2005.

[24] A. Atlas, A. Zinin, „Basic specifiaction for IP fast reroute: Loop-Free Alternates," RFC 5286, 2008.

[25] G. Rétvári J. Tapolcai, G. Enyedi, A. Császár, „IP Fast ReRoute: Loop Free Alternates Revisited", in Proc. IEEE INFOCOM, 2010.

[26] T. Čičić, „An upper bound on the state requirements of link-fault tolerant multi-topology routing," in IEEE ICC, vol. 3, pp. 1026-1031, 2006.

[27] G. Enyedi, G. Rétvári, T. Cinkler, „A novel loop-free IP fast reroute algorithm", in EUNICE, 2007.

[28] G. Rétvári, L. Csikor, J. Tapolcai, G. Enyedi, A. Császár, "Optimizing IGP Link Costs for Improving IP-level Resilience," to appear at DRCN, 2011.

[29] M. Nagy, G. Rétvári, "An Evaluation of Approximate Network Optimization Methods for Improving IP-level Fast Protection with Loop-Free Alternates", to appear at RNDM, 2011.

[30] B. Mazbic-Kulma and K. Sep, "Some approximation algorithms for minimum vertex cover in a hypergraph,"
in Computer Recognition Systems 2 (M. Kurzynski, E. Puchala, M. Wozniak, and A. Zolnierek, eds.), vol. 45 of Advances in Soft Computing, pp. 250–257, Springer Berlin / Heidelberg, 2007.

[31] L. Lovász, "On the ratio of optimal integral and fractional covers," Discrete Mathematics, vol. 13, no. 4, pp. 383–390, 1975.

[32] R. Mahayan, N. Spring, D. Wetherall, T. Anderson, "Inferring link weights using end-to-end measurements," in ACM IMC, pp. 231-236, 2002.

[33] SNDlib, "Survivable fixed telecommunication network design library," http://sndlib.zib.de.

[34] S. Knight, H. X. Nguyen, N. Falkner, R. Bowden, and M. Roughan, "The Internet Topology Zoo," http://www.topology-zoo.org.

ABOUT AUTHORS

Levente CSIKOR was born in 1986 and graduated at Budapest University of Technology and Economics in technical informatics in 2010. Now he is a second-year PhD student at the High Speed Networks Laboratory, Department of Telecommunications and Media Informatics, BME. He has experience in C/C++/LEMON, Java/JUNG, Linux, web development and databases. Currently he is involved in researching IP Fast ReRoute techniques, network optimization algorithms and heuristics to improve fast IP level resilience with Loop-Free Alternates.

Máté NAGY was graduated at Budapest University of Technology and Economics in electrical engineering in 2010. He spent a semester in Mikkeli University of Applied Sciences that raised up his interest in infocommunication. Now he is a software developer at Ericsson Magyarorszag Kft. and also takes part in researching IP FastReRoute solutions. He has experience in C/C++/LEMON, Java, Python and in Linux.

Gábor RÉTVÁRI received the M.Sc. and Ph.D. degrees in electrical engineering from the Budapest University of Technology and Economics (BME), Budapest, Hungary, in 1999 and 2007, respectively. He is now a Research Fellow at the High Speed Networks Laboratory, Department of Telecommunications and Media Informatics, BME. His research interests include QoS routing, Traffic Engineering and the networking applications of computational geometry and the mathematical theory of network flows. He is a Perl expert, maintaining numerous open source scientific tools written in Perl, C and Haskell.

Analysis of Identity Separation Against a Passive Clique-Based De-anonymization Attack

Gábor Gy. Gulyás and Sándor Imre

***Abstract*—Most of today's online social networking services have a flat structure, i.e., these services only allow a single choice of connection type (usually called "friends") for their users, and lack the functionality of identity separation. However, identity partitioning allows users to group their contacts, to share different or even diverse information, and therefore offer privacy protection against third parties looking to re-identify users in sanitized social graph data. In this paper, we analyze the protective strength of identity separation against these types of structural de-anonymization attacks by introducing a statistical user behavior model and defining attack failure probability formally. It turns out from simulations and the parameter analysis of the model that in case of even a relatively small number of users applying identity separation, an attacker is likely to fail.**

***Index Terms*—De-anonymization; Identity Separation; Social Network; Seed Identification.**

I. INTRODUCTION

A social network (SN) is a web of connections between certain individuals (or organizations) in the society, who are tied together by one or more specific relations or attributes, e.g., the trails of e-mails or phone calls altogether. The group of social networks includes social networking services (SNS), which allow individuals and other entities such as organizations to form links. These services have an underlying social network graph, where vertices represent individuals or registered users, and edges indicate relationships, connections or other kinds of links. Content on most SNSes is based on user-generated information, e.g., status messages, family photos and videos, and hyperlinks to other websites. Such services may also include the functionality of creating and joining groups of interest, and rating other users' content – a simple concept for which being Facebook's likes.

A social network is a rich information base for many branches of science. Sociologists, for instance, may find out valuable information about the structure of the society, group behavior, etc., by analyzing the *anonymized export* of the database, which can be considered a graph with labels on the vertices and edges, where vertices represent members of the network, and edges connection between them. Such an export may either be obtained through a request to the operator of the SNS, or by manually collecting the information through the use of a so-called web crawler.

Anonymization is not a trivial task; merely stripping the names from the database has proven to be insufficient [19]. An attacker may embark on restoring the deleted identifiers for various reasons, e.g., for obtaining previously unknown or unconfirmed information about a user for improving the efficiency of illegal or otherwise malicious practices, such as phishing. Research in the field has made such attacks against social networks readily available, and has proven that they do not have a prohibitively high complexity [20].

As a means of thwarting de-anonymization attempts, we propose to use identity separation in social networks [12], a concept for selectively concealing and revealing certain pieces of information in specific contexts, which is called the technique of Partial Identities [6] or Role-Based Privacy [12]. For instance, one may want to separate her colleagues from her friends (in the stricter sense of the word) on a SNS, by effectively managing separate contact lists for separate identities [11]. This concept, since it harmonizes with our real-life information sharing habits [2], is now available as built-in function, in a novel SNS, called Google+[2].

In this paper, we analyze the effectiveness of identity separation against de-anonymization attacks in case of a cooperative service provider (i.e., who leaves identities separated in the export; the analysis of the uncooperative service provider is considered as future work). These attacks can be categorized as active, semi-passive and passive methods. Active attacks allow creating new nodes in the social network, and adding edges with the rest before obtaining the anonymized export, while semi-passive attacks only allow creating additional edges without adding vertices [4]. Passive attacks rely on the unmodified content in the database, but use auxiliary data sources to de-anonymize users [20], [21].

Our work focuses on the state-of-the-art passive attack in [20]. Although the work described in [21] is more recent, but that attack is not proven to be generic: while the attack in [20] is executed on two totally different networks, namely Flickr and Twitter[3], the attack in [21] is executed on two snapshots of the same (Flickr) network. The latter attack has two significant disadvantages, since it tries to match the top l nodes in the two networks: first, due to its characteristics, it

Manuscript received August 16, 2011.

G. Gy. Gulyás is an adjunct assistant professor at the Department of Telecommunications, Budapest University of Technology and Economics. Magyar tudósok körútja 2., H-1117, Budapest, Hungary. (gulyasg@hit.bme.hu).

S. Imre is a professor, and the head of department at the Department of Telecommunications, Budapest University of Technology and Economics. Magyar tudósok körútja 2., H-1117, Budapest, Hungary. (imre@hit.bme.hu).

[2] http://plus.google.com

[3] http://flickr.com and http://twitter.com

could not work for another set of nodes with lower degrees, and second, matching the top l nodes in different networks may involve some difficulties (see Section II.A).

Therefore, as our main contribution in this paper, we have analyzed the success rate of the state-of-the-art attack from a user's point of view by calculating failure probability for a single vertex of the anonymized export. To assure the generality of our analysis – and since user behavior is yet unknown – we have defined a generic attack-independent statistical model for user behavior regarding identity separation and edge anonymization.

The paper is structured as follows. In Section II, we review the related literature on the main areas involved by our research: re-identification in anonymized social network graphs, identity separation and anonymity in social networks. In Section III, a novel user behavior model is introduced for identity separation, which incorporates multiple behavior types dependent on the possibilities of the user. The effects of identity separation on active attacks are discussed in Section IV, and in Section V, the analysis of passive de-anonymization attacks is presented. Finally, in Section VI, we conclude our work.

II. LITERATURE SURVEY

In this section, we briefly discuss the literature most related to our work. First by including the most relevant de-anonymization attacks, and also discuss the literature of identity separation for social networks. Finally, we present a method for applying anonymity in social networks, and for exporting such data.

A. De-anonymization Attacks for Social Networks

The first de-anonymization algorithms were active (and semi-passive) attacks [4]. As discussed in the introductory section, attacks of this type intend to insert a hidden but unique pattern into the graph by systematically adding vertices to the social network graph, and trying to create edges between some targeted users, before obtaining the anonymized export. The adversary may then attempt to recognize this hidden structure, and infer information about the selected users under attack (i.e., which are connected to the structure), including their contacts and (if provided along with the graph) their profiles.

However, since active attacks intrinsically assume that the adversary is able to modify the network before creating the export, they inherently have some weak spots. For instance, in case the modification is possible, the operator of a major social networking website is likely to attempt to find the fake user accounts, and delete them. Since real users of the social network do not have a meaningful motive to link back to the malicious nodes (i.e., confirm friend requests), the service provider will find that edges linked to these vertices are mostly going outwards from, and seldom coming inwards to them. The computational complexity of active attacks is likely to be small [4].

Passive attacks, while computationally more expensive, do not require the modification of the social network graph, and therefore the service provider cannot proceed with reactive measures, only with proactive ones. This makes the attack more difficult to counter, and also more versatile in terms of area of application (i.e., the same concept can be applied to multiple kinds of social networks). Furthermore, these attacks are capable of extending to the entire network, or at least a significantly large part thereof.

The state-of-the-art passive attack described in [20] maps the corresponding nodes of two graphs (i.e., accounts of the same person) solely based on structural information. The adversary defines an error parameter ε to control the acceptance of a mapping, i.e., if the algorithm should be more lenient and possibly accept erroneous mappings, or be stricter and be prone to rejecting correct ones.

The algorithm executes in two phases: seed identification and propagation. In the first phase, the attacker tries to find in the anonymized graph the counterpart of a unique k-clique present in the source graph (the algorithm in [20] uses 4-cliques, to be exact). First, for a unique k-clique in the source graph, the attacker computes the degree of each vertex and the number of common neighbors for each pair of nodes, then looks for similar k-cliques with similar values (within a factor of $1 \pm \varepsilon$) in the target graph. The error factor is considered for mapping each vertex (in the case of degrees) and each pair of vertices (in the case of common neighbor counts). Structural modifications within the cliques are disallowed; identification fails if one or more edges are erased from the clique.

In the second phase, the algorithm iteratively adds nodes to the mapping until there are unmapped vertices that have reasonably good mappings. If the attacker fails in the first phase, the second one is never run; therefore, we focused on analyzing the success rate of the attacker, but plan to analyze the effects of identity separation on this phase as future work. However, we expect that if the seed identification is not successful in general, then the second phase should fail, too.

Narayanan et al. in [21] introduce a similar attack with a less rigid, non-pattern-based seed identification phase (the propagation phase is essentially the same). Instead of looking for several seeds, this attack tries to find matches of node pairs in the top l nodes of the two networks, and then starts the propagation phase from there. Matches are based on node degrees and common neighbor counts by applying cosine similarity for the pairs.

However, this attacker algorithm does not seem to be generic. First, since degrees of nodes in the top l set differ the most in the whole network, this technique can not be applied to other set of l nodes with lower degrees: there would be too many similar nodes in the compared sets (e.g., see Fig. 1-2 in [21]). Second, for social networks with a similar purpose (e.g., Facebook[4] and Google+), it may be right to assume that the top l nodes overlap, but in general, that should not be true. For instance, it is not very likely that accounts belonging to the same owners are the most popular on Flickr and on LiveJournal.

Therefore, to the best of our knowledge, the [20] passive attack is still the state-of-the-art attack that can be found in the

[4] http://facebook.com

literature. Comparison of attack types are summarized in Table 1.

TABLE 1. ATTACK TYPES AND ATTACKER CAPABILITIES.

Data sources	Passive	Semi-passive	Active
External data	Use public data as auxiliary source		
Internal data	-	Modify profiles, connections	
	-	-	Create new registrations

B. *Identity Separation in Social Networks: a Desired and Privacy-Enhancing Feature*

We do not classify our social contacts on SNSes by default, as there is only one category: "friends". However, this is normally not the way we, humans, classify our acquaintances [2]. We keep track of multiple groups of people we know from different "stages" of our life, e.g., school, workplace, and family, and interact with them in a disjoint fashion in terms of place and time [8]. If our offline disclosure of information works in a different way than an SNS, we will act in a different way online: we will likely self-censor ourselves, and, at least sometimes, disclose some content to unwanted audiences.

This is a clear indication for the need of identity separation within social networks [11]; SNSes allowing users to share diverse information with different user groups (e.g., sharing different availability status with colleagues and friends) or to commit identity separation in some contexts (e.g., making political and private identities totally unlinkable). Such methods exist in the literature as the technique of Partial Identities [3], [5], [6], [10], [9], and Role-Based Privacy [24], [14], [15], [16], [18], [12]. Both allow users to publish diverse attributes under different pseudonyms.

For the case where the consent of the SNS provider cannot be assumed, one can use cryptography to enforce identity separation on an existing SNS [22], [1] or implement the social network on a distributed, cryptographically secured architecture [7]. However, our current work focuses on the possibilities on the model issues, and not the cryptographic side of the problem.

Google+ is the first to implement identity separation as a tool for privacy protection; the goal of this feature (namely Google Circles) is to allow proper audience selection for sharing content. Currently, this is not yet a complete solution, as it only works for content sharing, but there is only a single profile (flat structure). One important attribute of the Circles feature that it is mandatory.

Similar, optionally available features exist in many services. For instance, in the Windows Live Messenger[5], one can set invisible mode for each contact group separately, or in Facebook, friends can be sorted into groups, and content sharing can be done accordingly. Compared to the Google Circles, the biggest disadvantage of these features is that they are optional, and therefore probably fewer users know about and use them.

C. *Anonymity, Pseudonymous Identifiers and Data Export Sanitization*

There are two types of identity separation. The simpler identity separation function is where you can sort your contacts into lists, and, for instance, post content for them separately. This is called internal identity separation [11]. The other means of separating identities – external separation – is either managing multiple profiles on the same SNS, or using multiple networks for different audiences (e.g., Facebook as our means of informal online presence, and LinkedIn[6] as our formal one).

Obviously, the user's pseudonyms on different sites must not disclose that they belong to a single user [5]. It must be noted, too, that the internal separation functionality found on many SNSes is insufficient. For instance, Facebook does not allow hiding group memberships, implicitly exposing attributes of the user that she may have wanted to conceal [25].

Therefore, a social network supporting identity separation allows three levels of anonymity [12]:

- The weakest is pseudonymous identification (i.e., internal separation): the user is identified by a globally unique identifier (a pseudonym), and her identities can be linked through it.
- Unlinkable pseudonymity is a stronger level of anonymity (i.e., external separation), where the user may separate her identities by the means of multiple pseudonymous identifiers. These cannot be linked together, since content corresponding to an identity has its respective pseudonym as the originator.
- The strongest level is total anonymity, which allows the user to post content without any identifier linked to it, and therefore making it very hard to trace the information back to her.

In our work, we assume a service provider that honors the above mentioned separation methods when creating the network export. The reasoning behind this is that if the attacker cannot reverse the separation, she cannot know that multiple nodes in an anonymized graph belong to one person, and therefore they should be mapped together to a vertex in the known graph.

Transformation of a social network where the users can use identity separation and edge anonymization into a traditional social network graph is simple. Linkable nodes (i.e., those that use linkable pseudonymous identifiers) are merged, unlinkable nodes (i.e., those that use separate pseudonymous identifiers) are preserved as separate vertices, and anonymized edges are simply deleted. This way, all the aforementioned levels of anonymity in the privacy-enhancing social network model are reflected in the transformed graph. To sum it up, it can be seen that user behavior can greatly affect the structure of the exported social network graph.

[5] http://explore.live.com/windows-live-messenger

[6] http://linkedin.com

The original articles on passive attacks analyze scenarios where the source (or auxiliary) and target graphs were both regular social networks. In this paper we analyze a mixed scenario, where the source graph is a regular social network, and the target is one which allows identity separation. In this case, modeling user behavior is easy, since only the separation process needs to be approximated with a statistical model.

We leave the analysis of the third type of attacks, namely that uses networks with identity separation for both the source and the target, as future work. In this case pattern-based methods may also work; however, if there is no reference data on user awareness, it needs to be modeled. The reason for this is simple: for instance, a user that has a higher level of awareness may use different identities in the source and target networks to make such de-anonymization attacks more difficult to execute. Therefore, the success of these attacks is not as trivial as for the first type of attacks.

III. Modeling User Behavior for Identity Separation

In this section, we describe a model (a set of sub-models) of the user behavior for identity separation that allows all the three levels of anonymity mentioned in Section II.C. We have mapped identity separation to the graph model as "splitting" a vertex in a graph and probabilistically sorting the edges (represented connections with her contacts) between the new nodes, in some cases allowing duplication of edges with a certain probability. As mentioned before, anonymization of an edge is reflected by deleting it from the graph with a certain probability.

There might be other approaches for modeling user behavior; however, in our opinion this approach is the closest to how people manage their acquaintances in their lives [2]. Furthermore, just to mention a real-life example, our approach is quite similar to functionality in Google+, namely how contacts are managed in the circles feature.

Another important property of our model is that it is attack independent. This allows analyzing multiple attacks with this model, even pattern-based and other, non-pattern-based ones.

A. Modeling Identity Partitioning

Let us define a regular social network graph as $G_{SN} = G(V, E)$. Node $v \in V$ is a user who has $n = \deg(v)$ neighbors in G. While performing identity separation, node v introduces y new vertices (i.e., new identities), and sorts edges with probabilities $p_1,\ p_2, \dots, p_y$ to each of the new identities.

We can categorize the model parameters as:

- Context-dependent parameters: the user has little influence over such parameters. The only context-dependent item in our model is the neighborhood size of the user (n).
- User-dependent parameters: these are the statistical descriptors of user behavior. In our model, the number of new identities denoted as y and the probabilities of sorting edges ($p_1 \dots p_y$) can be considered as user-dependent parameters.
- Attacker-dependent parameters: the adversary is free to choose these before executing the de-anonymization attack. Currently, there are no such parameters (as the model is attack independent), but for instance, in Section V. such new parameters will be introduced.

The number of new identities (y) is modeled with a random variable Y. The distribution of the edge sorting is $P(X_1 = x_1, \dots, X_y = x_y)$, where X_i is a random variable describing the number of edges between the ith new identity and the neighbors of the original node. We do not assume any distribution for Y, and the distribution for X_i is defined with the chosen user-behavior model.

The model and the parameters could be fine-tuned with quality reference data; however, there are some obstacles in the way. As mentioned before, Google+ is the first service that compels its users to sort their contacts, and although the profiles are public, circles of users are not yet. Furthermore, in other services where sorting contacts is available but not mandatory, we experienced that this feature is rarely used, and often the contact groups are not publicly available – making social network data harvesting a futile task. Therefore, verifying our model with reference data is still an open research task that stays future work.

B. General Assertions

Our model is based on some assertions about the structure of the network before and after applying identity separation. These assertions are assumed to be true in all sub-models.

Assertion 1. *A new identity can have even zero of the original contacts in the export (i.e., due to edge anonymization).*

Assertion 2. *A user v_i may create a maximum of* $\deg(v_i)$ *new identities.* While it is possible to create an unlimited number of identities, and assign duplicate edges to them, we believe that this does not match with the user's expected behavior and this is an acceptable rational limitation.

Assertion 3. *A user may create even 0 new identities (i.e., perform self-deletion from the graph).* This happens when all the connections are anonymized.

Assertion 4. *The only contacts existing in the source network are modeled in the identity partitioning.* This simplifies the behavioral model, but does not necessarily make the results more favorable: including new contacts would add noise to the model, which would increase failure rates.

Assertion 5. *All actions of the nodes in the network are assumed to be using identity separation independently.* Our analysis does not cover collaborating users, even though collaboration would mean stronger resistance and higher failure rates.

Assertion 6. *Edges are not sorted independently.* This is a rational consideration, since all new identities belong to the same user, who sorts the edges (in an intelligent way).

C. Sub-Models for User Behavior

Dependent on the chosen user behavior, there are further aspects to be considered in the sub-models:

- Can different identities of the same user have overlapping neighborhood (i.e., duplicated edges)? Overlapping allows the overall number of connections to increase, formally, $\exists P(X_1 = x_1, \dots, X_y = x_y) > 0$, that $\sum x_i > n$ with $(0 \leq x_i \leq n)$.
- Is edge anonymization permitted? Deleting edges allows the overall number of connections to decrease, as $\exists P(X_1 = x_1, \dots, X_y = x_y) > 0$, that $\sum x_i < n$.

Based on these aspects, new sub-models can be introduced that we have summarized in Table 2. The names of the sub-models require some explanation. We have named the model with no edge anonymization, and no overlaps the basic model, since this allows the least privacy enhancing functionality for the user (only identity separation itself). Conversely, the realistic model is just the opposite: it implies the fewest limitations in her possibilities. We believe that most users of a social network would use anonymization or duplication for their connections; hence the notation "realistic".

TABLE 2. CATEGORIES OF MODELS OF USER BEHAVIOR.

	Overlap	**No overlap**
Edge deletion	Realistic model	Best model
No edge deletion	Worst model	Basic model

Besides, a worst and a best model also exist, which are named from the algorithm's point of view. The best model allows a user to only decrease the number of her contacts, and therefore causing more information loss (i.e., structural damage). The worst model is the opposite: it only allows creating duplications, and therefore making "backups" of structural information, and helping the attacker that way.

IV. IDENTITY SEPARATION AND ACTIVE ATTACKS

Backstrom et al. describe two attacks, a semi-passive and an active attack, in which both the attackers are able to modify the network prior to the sanitization [4]. In both attacks the attackers' goal is to insert a specific structure (a subgraph) into the SN graph that can be revealed later only by the attackers but no one else – this is what they call structural steganography. This subgraph is connected to the SN graph by creating new edges to a small number of targeted users. This is one the disadvantages of this attack: they only allow revealing the identity of a small number of users. However, for some networks active and semi-passive attacks can not be executed for one of the following reasons:

- The modification of the network structure may be expensive (e.g., phone calls).
- The modification may not be executable (e.g., network created from observed e-mails).
- To insert the structure too many modifications would be required (e.g., a valid e-mail address must be providing for the registration).
- The attacker is not always able to influence connections (e.g., connections require two-way confirmation).

All these problems inspired the research of passive attacks [20]. However, from the viewpoint of identity separation, the active attacks are better than passive attacks: the inserted structure is under the exclusive control of the attacker, and therefore its structure is always known, and can be found by the malicious collaborators. On the other hand, even if such attacks may not be prevented, one can use identity separation to separate herself from suspicious users, neighborhoods (i.e., structures) to prevent re-identification. This kind of self-defense works against passive attacks, too.

V. ANALYSIS OF FAILURE PROBABILITY FOR THE CLIQUE-BASED PASSIVE ATTACK

In this section, we discuss our results of the analyses based on the user behavior model in case of an attacker using the clique-based algorithm (discussed in Section II.A). We included an assumption from the original attack: there are some unique 4-cliques that exist in both networks and have similar neighborhoods in both, i.e., the cliques contain vertices with similar degrees [20].

Seed identification is considered to be successful for a clique if it remains a clique, and retains its degree values within an error factor after applying the identity separation. While the original algorithm compares common neighbor counts as well, our analysis concludes that even these two criteria can be violated effectively with identity separation, as shown later (i.e., we analyze the lower bound for the failure probability).

Here, we analyze the failure probability of the attacker on statistical basis; however, it should be noted that individual protection against attacks is still possible, even if statistically an attack seems to be feasible, i.e., a user can intentionally create different neighborhood structures in different networks.

In our opinion, the basic and the realistic models are the closest to real user behavior: we expect users to have roughly the same number of contacts before and after the identity separation (not including new contacts). Therefore, in our research, we focused on these models: the basic model is an analytically simpler model allowing identity separation only, and the realistic model allowing more functionality for users (with more mathematical complexity).

A. Naïve Analysis on 4-cliques

By using real-life data harvested from different social networks, we simulated identity separation to analyze its effects on the network structure from the attacker's clique-oriented point of view. Cliques can be easily destroyed via identity separation:

- One of the users separates herself totally from the clique. This is equivalent to the removal of the representing node.
- One of the users removes at least one edge from the clique.
- At least one of the users uses identity separation and separates at least an edge from the clique.

In these cases, the clique no longer remains connected, and the attacker will fail in finding it. We executed simulation experiments to determine how effectively identity separation removes 4-cliques from the network. For our experiments we used structural information crawled from two real-life networks: the Slashdot friend or foe links that were crawled in February 2009 [17], and the Epinions who-trust-who network data that were crawled in 2003 [23]. From the Slashdot network 10,000 nodes were selected containing 1,816,110 4-cliques, and 1,000 nodes were selected containing 2,102,842 4-cliques from the Epinions network. For comparison, a full graph of 100 nodes (with 3,921,225 4-cliques) was also included.

For simulating identity separation, random nodes were selected to be split into two new nodes, and edges were assigned to each with equal probability (i.e., accordingly to the basic model). We have also defined a theoretical limit to show the expected number of cliques affected by identity separation. Adding more privacy-enhancing functionality to the simulation, such as edge and node removal, the number of cliques would be furthermore decreased, closer to the theoretical limits.

If random variable Y denotes the number of identities belonging to the same user (without assigning a distribution to it), the probability if there are any identity separations in a k-clique $C_k = \{v_1, \dots, v_k\}$ can be calculated as in

$$p_{ids} = P(\exists v_i: Y_i > 1 \mid i = 1..k) = 1 - P(\forall v_i: Y_i = 1 \mid i = 1..k) = 1 - P^k(Y = 1). \quad (1.)$$

Therefore, the expected number of cliques remaining intact can be calculated as the expected value of the binomial distribution $Z \sim B(N_{kcls}, 1 - p_{ids})$, where N_{kcls} denotes the number of 4-cliques in the original graph. The expected value of Z is

$$E[Z] = N_{kcls} \cdot (1 - p_{ids}) = N_{kcls} \cdot P^k(Y = 1). \quad (2.)$$

The relative values of $E[Z]$ with $k = 4$ are denoted on Fig. 1 as the expected number of cliques remaining intact by identity separation (denoted as "Theoretical"). It is possible that the clique remains a clique, but the probability of recovery depends on further errors regarding the compared degree and common neighbor count values. An analysis of these issues is discussed in the next sections.

We found that as the number of users who use identity separation increases, the number of 4-cliques decreases fast and almost similarly for all networks (see Fig. 1). For instance, in both test networks for $P(Y = 2) = 0.2$ the number of remaining cliques was almost halved: the percentage of intact 4-cliques was 52.26% for the Slashdot network, 51.27% for the Epinions network, and 55.22% for the full graph. It is also visible on Fig 1. that graphs having more 4-cliques degrade faster. The reason behind this phenomenon is simple: usually several 4-cliques overlap in a single node, and therefore splitting it causes the deletion of multiple 4-cliques.

Our conclusion is for the naïve analysis: identity separation erodes network structure effectively, thus it offers strong protection against structural attacks, and therefore it needs to be furthermore analyzed.

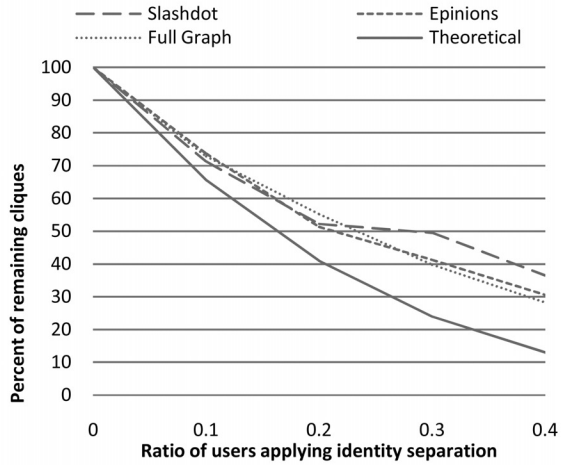


Fig. 1. Simulation results (including the theoretical limit) show the degradation in clique numbers in case of allowing identity separation.

B. User Behavior Model with Attack Related Parameters

In this case, node $v \in V$ is a user who is part of a k-clique, and has $n = \deg(v)$ neighbors in G, and therefore node v has $k - 1$ inner and $n - k + 1$ outer edges, as seen from the viewpoint of the clique.

For the inner edges, the distribution of the edge sorting is described as $P(X_1 = x_1, \dots, X_y = x_y)$, with no predefined distribution included; the distributions are defined with the chosen model. For the outer edges, the distribution is described similarly as $P(X'_1 = x'_1, \dots, X'_y = x'_y)$. X_i and X'_i are random variables describing the number of edges between the ith identity and the members of the original clique, and those between the ith identity and the neighbors of the original node, respectively.

The original algorithm defines an error parameter ε for the seed identification, and an error measure based on it: the matched node degree values need to match within an error factor of $1 \pm \varepsilon$.

Based on this, we define an error measure function that will be used in the calculation of the failure probability, given by the function of

$$g(x, y) = \begin{cases} 1, \left(\frac{x+y}{n} < 1 - \varepsilon \wedge y = k - 1\right) \vee y < k - 1 \\ 0, \text{otherwise} \end{cases}, \quad (3.)$$

where x denotes the number of outer, and y denotes the number of inner edges.

The node degree value n, the clique size k, and the error parameter ε are assumed to be known constants. We note, that the clique size (k) and the error parameter (ε) are new attacker-dependent parameters introduced to the model (see Section III.A). It should be noted that the attacker, to achieve better results, can choose to execute several attacks with different values for these parameters, without any limitations.

C. Calculation of Failure Probability

It must be noted that different actors have different views on the measure of failure probability. The adversary is interested in discovering the correct mapping for several cliques. As such, she is likely to be interested in the probability of failure in identifying a k-clique. Here, we only define the failure probability for a single node, but for a clique it can be calculated simply by giving the probability of the union of failure events, where members of the clique damage the clique or change node degree values and causing errors.

The point of view of a user is, on the other hand, that she herself should not be vulnerable to the attack; other users are more or less irrelevant to her. This is why we have focused on calculating failure probability of single users. It must be noted that this probability is clique-independent, and therefore the same regardless of the number of cliques the user is member of.

Furthermore, the calculation does not take actions of other users in the clique into account, i.e., it is assumed that they neither perform identity separation, nor anonymize any of their edges. If we took these effects into account, the failure probability would be higher in most cases, and at least equal in theory, since other users could also destroy the clique or change the degrees of the vertices thereof, making identification less probable.

The probability of failure for a node v_a, based on the variables, assumptions and assertions introduced previously is

$$P(\text{"fail for } v_a\text{"}) = P(Y=0) + \sum_{y=1}^{\deg(v_a)} P(\text{"fail"}|Y=y)\cdot P(Y=y). \quad (4.)$$

The first member of the sum is the probability of the case where the user has 0 identities in the exported graph, i.e., all her edges are anonymized. The other part of the sum incorporates Assertion 2, namely that the user creates at most as many identities as many contacts she has. The results for the different sub-models of user behavior mainly deviate in the definition of the conditional probability $P(\text{"fail"}|Y=y)$. Note that the formula for the sum may slightly differ in some cases, e.g., in that of the basic model, where it does not include probabilities for $y=1$.

In the general case, the conditional failure probability in (4) can be unfolded as

$$P(\text{"fail"}|Y=y) = \sum_{\forall l_i} P(\text{"fail"}|X_1=l_1,\dots,X_y=l_y)\cdot P(X_1=l_1,\dots,X_y=l_y). \quad (5.)$$

Furthermore, probability $P(\text{"fail"}|X_1=l_1,\dots,X_y=l_y)$ can be calculated differently for two cases. If $\forall l_i < k-1$, i.e., the clique is always destroyed, since all edges are sorted in groups having less than $k-1$ edges, then $P(\text{"fail"}|X_1=l_1,\dots,X_y=l_y)=1$ always.

In the other case, where $\exists l_i = k-1$, the conditional failure probability in (5) is calculated as

$$P(\text{"fail"}|X_1=l_1,\dots,X_y=l_y) = P\left(\bigcup_{\forall m_i}(X'_1=m_1,\dots,X'_y=m_y|g(m_1,l_1)=1,\dots,g(m_y,l_y)=1)\right) \quad (6.)$$

By knowing that these events are mutually exclusive, (6) equals to

$$\sum_{\forall m_i} P(X'_1=m_1,\dots,X'_y=m_y)\cdot g(m_1,l_1)\cdot\dots\cdot g(m_y,l_y). \quad (7.)$$

Therefore, the failure probability for a node with y identities is

$$P(\text{"fail"}|Y=y) = \sum_{\exists l_i=k-1} P(X_1=l_1,\dots,X_y=l_y) + \sum_{\exists l_i=k-1} P(X_1=l_1,\dots,X_y=l_y) \cdot\left(\sum_{\forall m_i} P(X'_1=m_1,\dots,X'_y=m_y)\cdot g(m_1,l_1)\cdot\dots\cdot g(m_y,l_y)\right) \quad (8.)$$

This is applicable for any $y \neq 0$ number of identities, and by using this formula the overall failure probability can be described accordingly.

D. Failure Probability in the Basic Model

The basic sub-model is the analytically the simplest one, and the results obtained with this restricted model are quite satisfactory. The basic model introduces additional assertions.

Assertion 7. *Contacts of the separated identities do not overlap.*

Assertion 8. *Edges cannot be anonymized.*

In this model, the user sorts n edges among y identities. The multinomial distribution is a natural choice for describing such a case, since it describes n trials when the outcomes can be sorted into one of y groups. Additionally, group probabilities can be adjusted, and therefore this model allows fine-tuning the distribution in a way for describing user behavior in the desired way. Multinomial distribution is used as

$$P(X_1=x_1,\dots,X_y=x_y)\sim Mu(k-1,p_1,\dots,p_y), \text{ and}$$
$$P(X'_1=x'_1,\dots,X'_y=x'_y)\sim Mu(n-k+1,p_1,\dots,p_y),$$

where $\sum p_i = 1$.

The formula for failure probability can then be derived as:

$$P(\text{"fail"}|Y=y) \tag{9.}$$
$$= \sum_{\substack{\sum l_j=k-1 \\ \exists l_j=k-1}} \Bigg(P\big(X_1=l_1, X_2=l_2, \dots, X_j=l_j, \dots, X_y=l_y\big) \cdot \Bigg(\sum_{m_1=0}^{n-k+1} \cdots \sum_{m_{y-1}=0}^{n-k+1-\left(\sum_{h=1}^{h=y-2} m_h\right)} P\Big(X_1'=m_1, X_2'=m_2, \dots, X_j' = m_j, \dots, X_y' = n-k+1-\Big(\sum_{h=1}^{h=y-1} m_h\Big)\Big) \cdot g(m_j, l_j)\Bigg)\Bigg)$$
$$+ \sum_{\substack{\sum l_j=k-1 \\ \nexists l_j=k-1}} P\big(X_1=l_1, X_2=l_2, \dots, X_y=l_y\big).$$

Then, the overall failure probability can then be derived easily. We know that for $P(\text{"fail"}|Y=1)$ the neighborhood of the node would remain the same, and therefore would not introduce any error in the seed identification. Consequently, the result can be deduced from the general formula, with the exclusion of the case for $y = 1$.

During our numerical analysis, we have found that in this model for a fixed p_1, the failure probability for two identities is the lower bound for all failure probabilities with a higher number of identities that include p_1. In other words, for $\forall p_1, \dots, p_k$ with a fixed p_1:

$$P(\text{"fail"}|Y>2) \geq P(\text{"fail"}|Y=2). \tag{10.}$$

This is an important finding for two reasons. On the one hand, this is a lower bound for failure probability, and therefore it is enough to continue analysis in the case of $P(\text{"fail"}|Y=2)$. On the other hand, it facilitates the estimation of the overall failure probability as well:

$$P(\text{"fail"}) \geq \sum_{m=2}^{\deg(v_i)} P(\text{"fail"}|Y=m) \cdot P(Y=m) \tag{11.}$$
$$\geq \sum_{m=2}^{\deg(v_i)} P(\text{"fail"}|Y=2) \cdot P(Y=m)$$
$$= P(\text{"fail"}|Y=2) \cdot \big(1 - P(Y=0) - P(Y=1)\big).$$

Fig. 2 describes how failure probability changes with different values for parameter n, while parameters $k = 4$ and $\varepsilon = 0.05$ are fixed.

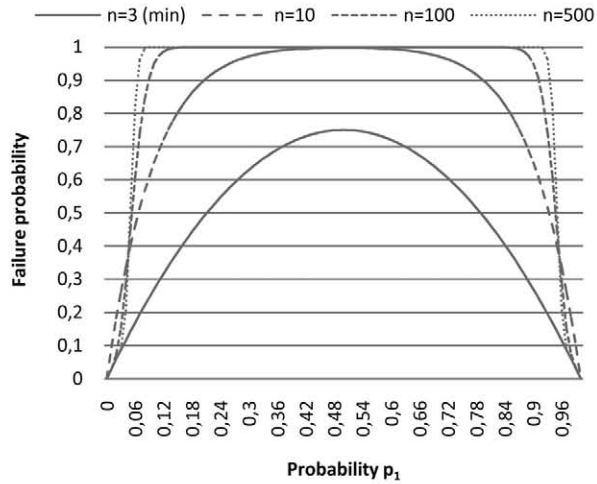


Fig. 2. Parameter analysis of n: $P(\text{"fail"}|Y=2)$ as a function of p_1, with fixed $c = 4$ and $\varepsilon = 0.05$ with different values for n.

The analysis has several interesting consequences. First of all, it can be seen that the failure probability is conveniently high even for a small n (e.g., $n \geq 10$). Secondly, users are given a relatively wide range of options for making their identification fail. Even if they use identity separation for just two identities, and the probability of using the second identity is small, the failure probability still remains high (e.g., for $p_1 = 0.1, n = 50$: $P(\text{"fail"}|Y=2) = 0.899$). It can be seen that the curve has inflection points. These are functions of the error parameter ε.

Fig. 3 describes how the failure probability changes in the function of ε while parameters $n = 100$ and $k = 4$ are fixed. The curves do not deviate significantly for other n values either.

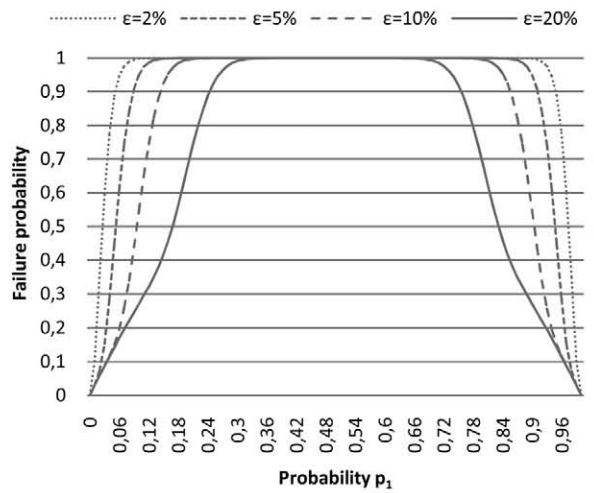


Fig. 3. Parameter analysis of ε: $P(\text{"fail"}|Y=2)$ as a function of p_1, with fixed $c = 4$ and $n = 100$ with different values for ε.

This shape of the curve practically concludes that a user making use of identity separation in a meaningful way, the adversary cannot influence the success of the attack. It is demonstrated in the original article that the value of ε should

be around 0.05, and that a practical limitation of $0 < \varepsilon \leq 0.1$ applies. For these values, users should choose p_1 and p_2 such that $0.1 \leq p_1, p_2 \leq 1$ $(p_1 + p_2 = 1)$, because this marks a point (i.e., a failure probability) beyond the inflection point of the curve. Finally, the analysis of parameter k has shown that there is no deviation in the failure probability for different clique sizes with different neighborhood sizes (n with $\varepsilon = 0.05$).

To sum it up, we can conclude that if the users use identity separation wisely, considering the influencing power of different parameters as mentioned above, the attacker has a low probability of identifying the nodes. This means that users need to separate their contacts into larger, but not necessarily equally sized groups. Therefore, this user behavior model can be suggested for users as a practical way to use identity separation, since it offers powerful protection if applied widely throughout the network.

E. Analysis of the Realistic Model

In this section, we discuss the analysis of the realistic model, which deviates from the basic model in regard of the additional Assertions 7 and 8.

Assertion 9. *Contacts of separated identities can overlap.*

Assertion 10. *Edges may be anonymized by users.*

Selecting the proper distribution is not an easy choice, therefore it should be defined by its probability matrix, denoting the probability of a possible outcome in a cell. Deciding which distribution to choose in such a model is an interesting question. In our opinion, the distribution should reflect that the most likely case is that the number of all contacts after the identity separation is similar to that before, i.e., a few deletions and duplications are likely, but major deviations are not (see Fig. 4).

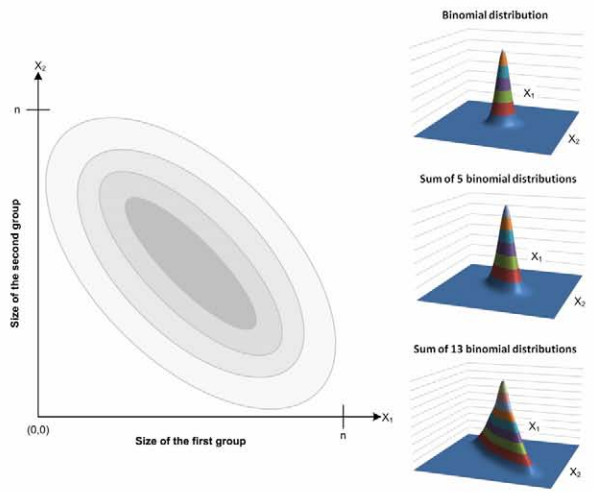


Fig. 4. Concept for the distribution of realistic models with $y = 2$, and some examples. On the left part of the figure, the darker areas have higher probabilities (these values are outstanding on the right part).

Accordingly to the given distributions and the generic formulae for failure probability, we have done the parameter analysis numerically. Its characteristics are similar to that of the basic model, and the preliminary results are satisfactory for this model, too (see Fig. 5).

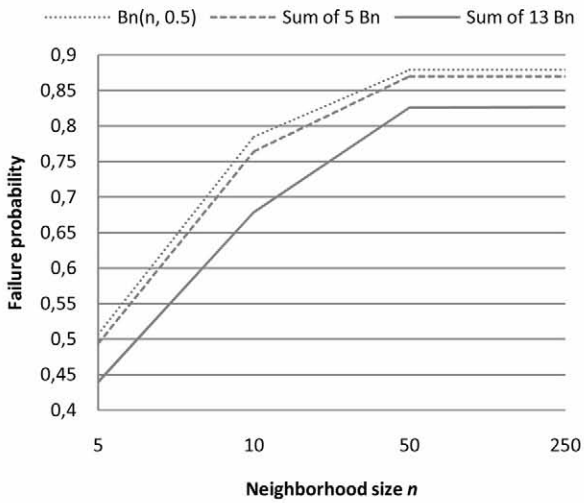


Fig. 5. Failure probabilities for different distributions with $y = 2$, for different sizes of n.

We can conclude that the results are satisfactory even for small ns in all distributions under examination; however, these models deserve further research dependent on reference data, which we assign as future work.

VI. CONCLUSION AND FUTURE WORK

Our analysis has shown that our proposed models make seed identification fail with high probability. Therefore, we can consider identity separation as an effective countermeasure against de-anonymization attacks if the user chooses the parameters wisely.

However, besides the answered questions, new ones arise. In the future, we would like to extend our analysis to the best and worst models, and discuss further results with the realistic model including new distributions compared with reference data if possible.

As it is mentioned in this paper, the analysis focused on the seed identification phase in the state-of-the-art passive attack, but the propagation phase should be analyzed in the future, since it is incorporated in two passive attacks [20] and [21].

It also seems to be desirable to extend the user behavior and the attacker model with new parameters to make it open for new attacks yet unknown. For example, the model can be extended to allow the analysis of the attack in [21].

Additionally, there are other types of third party attacks in the literature, such as attribute based ones [13], for which the effects of privacy-enhancing identity management should be analyzed. Instead of standalone use for re-identification, attributes can also be used to strengthen structural attacks: de-anonymization results can be easily verified and corrected by inspecting the available attributes of nodes. Perhaps identity separation has also a viable effect on these attacks – it would be interesting to see this in the future.

ACKNOWLEDGMENT

We would like to thank András Telcs for his valuable comments and suggestions on our work, and Ádám Máté Földes for inspiring discussions on the topic, and his suggestions during writing this paper.

Our work presented in this paper was supported from the KMOP-1.1.2-08/1-2008-0001 project by the BME-Infokom Innovátor Nonprofit Kft.

REFERENCES

[1] J. Anderson, C. Diaz, J. Bonneau, and F. Stajano, "Privacy-enabling social networking over untrusted networks," in *Proc. of the 2nd ACM workshop on Online social networks*, Barcelona, Spain, 2009, pp. 1-6.

[2] P. Adams, "The Real Life Social Network", presented at the Voices that Matter Web Design Conference, June 28-29, 2010, San Francisco, USA. Available at: http://www.slideshare.net/padday/the-real-life-social-network-v2

[3] K. Borcea, H. Donker, E. Franz, K. Liesebach, A. Pfitzmann, and H. Wahrig, "Intra-Application Partitioning of Personal Data," in *Proc. of Workshop on Privacy-Enhanced Personalization*, Edinburgh, UK, 2005.

[4] L. Backstrom, C. Dwork, and J. Kleinberg, "Wherefore Art Thou R3579X? Anonymized Social Networks, Hidden Patterns, and Structural Steganography," in *Proc. of the 16th international conference on World Wide Web*, Banff, Alberta, Canada, 2007, pp. 181-190.

[5] K. Borcea-Pfitzmann, E. Franz, and A. Pfitzmann, "Usable presentation of secure pseudonyms," in *Proc. of the Workshop on Digital identity management*, Fairfax, USA, 2005, pp. 70-76.

[6] S. Clauß, D. Kesgodan, and T. Kölsch, "Privacy enhancing identity management: protection against re-identification and profiling," in *Proc. of the Workshop on Digital identity management*, Fairfax, USA, 2005, pp. 84-93.

[7] L. A. Cutillo, R. Molva, and T. Strufe, "Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust," *IEEE Communications Magazine*, vol. 47, no. 12, pp. 94-101, Dec. 2009.

[8] J. M. DiMicco, and D. R. Millen, "Identity management: multiple presentations of self in facebook," in *Proc. of the ACM 2007 International Conference on Supporting Group Work*, Sanibel Island, Florida, USA, 2007, pp. 383-386.

[9] E. Franz, and K. Liesebach, "Supporting Local Aliases as Usable Presentation of Secure Pseudonyms," in *Proc. of the 6th International Conference on Trust, Privacy and Security in Digital Business TrustBus*, Linz, Austria, 2009, pp. 22-31.

[10] E. Franz, C. Groba, T. Springer, and M. Bergmann, "A Comprehensive Approach for Context-dependent Privacy Management," in *Proc. of the 2008 Third International Conference on Availability, Reliability and Security*, Barcelone, Spain, 2008, pp. 903-910.

[11] S. Gürses, R. Rizk, and O. Günther, "Privacy Design in Online Social Networks: Learning from Privacy Breaches and Community Feedback," in *Proc. of 29th International Conference on Information Systems*, Paris, France, 2008.

[12] G. Gy. Gulyás, R. Schulcz, and S. Imre, "Modeling Role-Based Privacy in Social Networking Services," in *Proc. of Third International Conference on Emerging Security Information, Systems and Technologies*, Athens, Greece, 2009, pp. 173-178.

[13] D. Irani, S. Webb, K. Li, and C. Pu, "Large Online Social Footprints – An Emerging Threat," in *Proc. of the 2009 International Conference on Computational Science and Engineering*, Washington, USA, 2009, Volume (3), pp. 271-276.

[14] U. Jendricke and D. Gerd tom Markotten, "Usability meets security - The Identity-Manager as your Personal Security Assistant for the Internet," in *Proc. of the 16th Annual Computer Security Applications Conference*, New Orleans, USA, 2000, pp. 334-344.

[15] J. Hakkila, and I. Kansala, "Role based privacy applied to context-aware mobile applications," in *Proc. of IEEE International Conference on Systems, Man and Cybernetics*, Hague, Netherlands, 2004, Volume (6), pp. 5467-5472.

[16] M. Hansen, A. Schwartz, and A. Cooper, "Privacy and Identity Management", *IEEE Security and Privacy*, vol. 6, no. 2, pp. 38-45, Mar/Apr. 2008.

[17] J. Leskovec, K. J. Lang, A. Dasgupta, and M. W. Mahoney, "Community Structure in Large Networks: Natural Cluster Sizes and the Absence of Large Well-Defined Clusters,". Tech. Rep., Preprint: arXiv:0810.1355, 2008.

[18] R. Leenes, J. Schallaböck, and M. Hansen, "PRIME white paper (V3)", May 2008. Available: https://www.prime-project.eu/prime_products/whitepaper/

[19] A. Narayanan, and V. Shmatikov, "Robust De-anonymization of Large Sparse Datasets," in *Proc. of the 29th IEEE Symposium on Security and Privacy,* Oakland, California, USA, 2008, pp. 111-125.

[20] A. Narayanan, and V. Shmatikov, "De-anonymizing social networks," in *Proc. of the 30th IEEE Symposium on Security and Privacy,* Oakland, California, USA, 2009, pp. 173-187.

[21] A. Narayanan, E. Shi, and B. I. P. Rubinstein, "Link Prediction by De-anonymization: How We Won the Kaggle Social Network Challenge," in *Proc. of the 2011 International Joint Conference on Neural Networks*, San Jose, California, USA, 2011.

[22] T. Paulik, Á. M. Földes, and G. Gy. Gulyás, "BlogCrypt: Private Content Publishing on the Web," in *Proc. of the Fourth International Conference on Emerging Security Information, Systems and Technologies*, Venice, Italy, 2010, pp. 123-128.

[23] M. Richardson, R. Agrawal, and P. Domingos, "Trust Management for the Semantic Web," in *Proc. of the 2nd International Semantic Web Conference,* Sanibel Island, Florida, USA, 2003, pp. 351-368.

[24] M. Reichenbach, H. Damker, H. Federrath, and K. Rannenberg, "Individual Management of Personal Reachability in Mobile Communication," in *Proc. of the 13th International Information Security Conference*, Copenhagen, Denmark, May 1997, pp. 164-174.

[25] E. Zheleva, and L. Getoor, "To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles," in *Proc. of the 18th international conference on World Wide Web*, Madrid, Spain, 2009, pp. 531-540.

Gábor György Gulyás received his M.Sc. degree in Computer Engineering in 2007, and now currently an adjunct assistant professor at the University of Technology and Economics (BME), Department of Telecommunications. He is a student member of the IEEE, and the Mobile Communications and Computing Laboratory (MC2L). He is one of the founders, and the moderator of the only Hungarian portal on Privacy Enhancing Technologies, the PET Portal & Blog. The focus of his research interests is on applying privacy-enhancing identity management to social networks, but he is also interested in the following topics: privacy and security issues of social networks, web privacy, data protection issues, and using steganography for enhancing privacy.

Sándor Imre was born in Budapest in 1969. He received the M.Sc. degree in Electrical Engineering from the Budapest University of Technology (BUTE) in 1993. Next he started his Ph. D. studies at BUTE and obtained dr. univ. degree in 1996, Ph.D. degree in 1999 and DSc degree in 2007. Currently he is carrying his activities as Professor and Head of Dept. of Telecommunications. He is Chair of Telecommunication Scientific Committee of the Hungarian Academy of Sciences. He participates the Editorial Board of two journals: Infocommunications Journal and Hungarian Telecommunications. He was invited to join the Mobile Innovation Centre as R&D director in 2005. His research interest includes mobile and wireless systems. Especially he has contributions on different wireless access technologies, mobility protocols, security and privacy and reconfigurable systems.

A Multi-disciplinary Approach to Lower Community Aircraft Noise Annoyance

F. Márki, M. Bauer, D. Collin, U. Müller, K. Janssens, U. Iemma

Abstract—**This paper presents the methods and tools of the 7th Framework European project COSMA (Community Oriented Solutions to Minimize aircraft noise Annoyance). COSMA aims to develop engineering criteria for aircraft design and operations in order to reduce the annoyance within airport communities due to aircraft exterior noise. By today, such criteria do not exist since aircraft noise engineering has historically focused on achieving ever lower noise levels for individual events and at close distance from the runway.**

Within the frame of a unique approach, COSMA will improve the understanding of noise annoyance effects due to aircraft in the airport surrounding community. The results from field studies and psychometric testing will be used for setting up optimised aircraft noise shapes. Special techniques for a realistic synthesis of aircraft noise around airports will be developed for the simulation and validation of optimised aircraft noise shapes. Associated engineering guidelines for the necessary optimisation processes will be established, which needs a profound knowledge management for aircraft design practices and scientific information on aircraft exterior noise annoyance effects. The scientific research results will help to reduce noise annoyance at the source in the future, by technological or operational means and through an improved understanding of the related effects of aircraft noise in the airport surrounding community.

Index Terms—**aircraft, annoyance, flight-path optimisation, noise, sound engineering, virtual resident**

I. INTRODUCTION

NOISE pollution from air traffic is a major environmental problem affecting airport communities. Aircraft flyover noise represents a complex auditory scenario wherein many acoustic, psycho-acoustic parameters other than loudness but also plenty of non-acoustical parameters affect the annoyance perception.

Manuscript received November 30, 2011. The partial financial support by the EU Framework 7 (funded under EC Grant Agreement ACP8-GA-2009-234118) has to be acknowledged.

F. Márki is with Budapest University of Technology and Economics (BME), Department of Telecommunications, Laboratory of Acoustics, Magyar Tudosok krt. 2., 1117 Budapest, Hungary (corresponding author, email: marki@hit.bme.hu).

M. Bauer is with EADS Innovation Works, CTO IW SP NA, 81663 Munich, Germany.

D. Collin is with SNECMA, Site de Villaroche Rond-Point René Ravaud, 77550 Moissy Cramayel, France.

U. Müller is with Deutsches Zentrum für Luft- und Raumfahrt e.V. (DLR), Institut für Luft- und Raumfahrtmedizin, Abt. Flugphysiologie, Linder Höhe, 51147 Köln, Germany.

K. Janssens is with LMS International, Interleuvenlaan 68, 3001 Leuven, Belgium.

U. Iemma is with Università degli Studi Roma Tre (UNIROMA TRE), Dipartimento di Ingegneria Meccanica e Industriale, via della vasca navale 79, 00146 Roma, Italy.

In order to investigate this, the EU FP7 project "COSMA" (Community Oriented Solutions to Minimise aircraft noise Annoyance) was started in 2009. The key elements of the multi-disciplinary approach to tackle noise annoyance include field studies more detailed than ever, to better understand annoyance and to serve as a basis for the so called Virtual Resident, Sound Synthesiser Machine examinations by lay participants for the creation of better-sounding aircraft, single- as well as multi-event flyover optimisation for quieter procedures, laboratory examinations for testing future aircraft sounds, procedures and airport scenarios. Aircraft manufacturers, sound engineering specialists, psychologists, acousticians, physicists, statisticians – a colourful team of specialists will all contribute to reach the goals of COSMA.

The present paper will first give an overview on the whole project workflow, followed by the detailed description of each major work-task. Not also the actual work tasks but also those methods to be developed in the project will be presented, which will give significant contribution to aircraft noise annoyance/abatement know-how of the state-of-the art research.

II. APPROACH OVERVIEW

In Fig. 1 a simplified overview of the project can be seen. Two heavy resource-demanding activities must first be described in order to understand the follow-up activities: i) telephone interview and field studies are performed to investigate current annoyance situations around airports and ii) beginning from the synthesis of a single flyover, complete airport scenarios must be synthesised to be able to analyse the effect of optimised aircraft sounds, take-off/landing procedures and airport scenarios.

The information gathered from the field studies are used to build a Virtual Resident, a tool to predict human annoyance on the basis of a set of parameters, like number of aircrafts, noise levels, etc. at a given observation point together with other factors that influence annoyance (so-called moderators) like expectation of future aircraft noise, procedural fairness, economic dependency from the airport etc. On the other hand, synthesised sounds are tested in laboratory examinations to see the level of their effectiveness.

The following items seen in Fig. 1 will be discussed in more details in Section III:

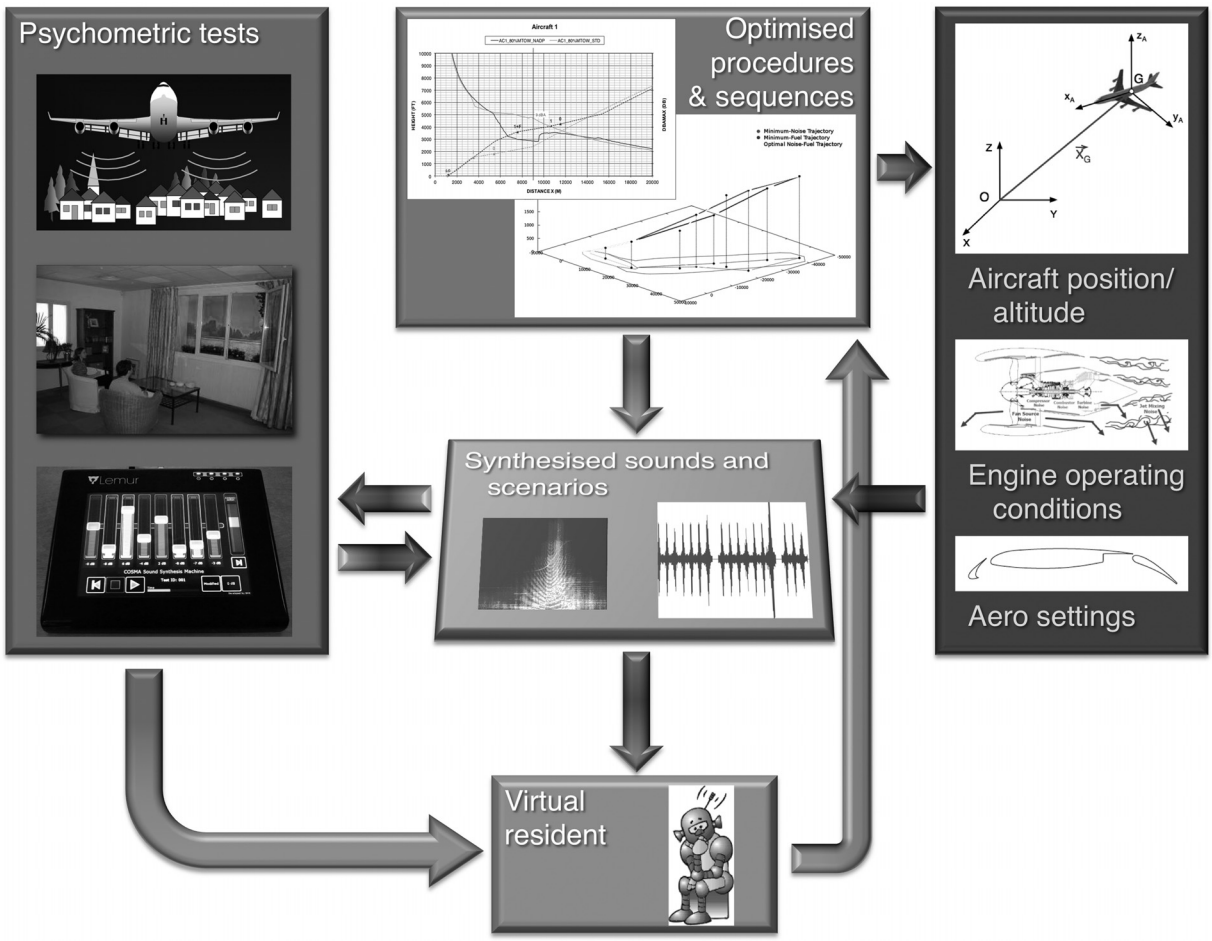


Fig. 1. Simplified workflow of the FP7 European Project COSMA. By making use of flight-path and sequence optimisation as well as application of psychometric examinations to create less disturbing aircraft sounds, sequences are synthetized. These sequences are tested in laboratory with lay participants to check the level of benefit of the optimisation. On the other hand, highly sophisticated field studies are carried out to analyse current situations around airports. The high number of hours spent by the participants in test allow an extensive exploitation of current situations, so a Virtual Resident model can be built, which is able to estimate human annoyance. The VRes will identify most annoying factors, which can be used as later

A. *Psychometric testing*

Four different kinds of examinations are performed in the work group responsible for psychometric examinations:

Telephone interviews & field studies

Telephone interviews allow studying what are the key moderators of aircraft noise annoyance around a specific airport. They form the basis for the development of the examination methods used in the field studies.

The real-life annoyance can only be tested in the field, in the houses of airport residents, during their regular daily activities. Participants fulfilling a set of requirements are invited to take part in the examinations. During 4 consecutive days, participants give their annoyance rating each hour, whilst the outdoor noise level is measured continuously. Additional questions each hour and before and after the whole testing days allows gathering information about non-acoustical moderators which strongly influence actual annoyance.

Laboratory studies

The laboratory studies allow to test 45 minutes sequences one against the other. Two benefits are to be mentioned here: i) the same scenario is tested by several participants (which is a big advantage in statistical analysis, but is not the case for field studies), ii) future aircraft/airport scenarios can be presented to the participants.

Sound Synthesiser Machine examinations

It is of high difficulty for lay people to express what are the most disturbing sound-features of an aircraft flyover and how much one or the other component should be modified to come to a better sounding aircraft. The Sound Synthesiser Machine is a unique tool to overcome these difficulties: faders are assigned to different aircraft components, like tones, engine-noise, etc., and by moving the faders, one can easily create less disturbing flyover sounds.

B. *Optimisation of procedures and sequences*

This part of the project addresses the possible benefit of other take-off/landing procedures, as well as the optimisation of aircraft types in respect of a few parameters (like constant number of passenger movements in a given time period, etc.). The optimisation results are directly used in the sound engineering workgroup.

C. Sound engineering

The realistic-sounding synthesis of aircraft flyovers and sequences play an important role in the exploitation of future aircraft, manoeuvres and sequences. Two kinds of sound engineering tools are realised in the project: i) an online "Sound Synthesis Machine" for lay people (e.g. for non-engineers or specialists in the field of aircraft industry) to find optimal-sounding aircraft sounds and ii) an "Aircraft Noise Climate Synthesiser" for sound engineering specialists to synthesise from the ground aircraft flyovers/sequences according to any aircraft assembly, flight-path, manoeuvre parameters. This latter is also used to synthesise those sequences and procedures specified by the optimisation work group.

D. Virtual Resident

This highly sophisticated tool will contain and use as much knowledge as possible to predict the most probable human annoyance reaction to an unknown aircraft sequence. The examinations performed in COSMA will serve as a starting point, but it is intended to develop the tool so that results of future field studies can also be included in it.

III. KEY STEPS IN FINDING SOLUTIONS TO LOWER COMMUNITY AIRCRAFT NOISE ANNOYANCE

Not only an overview was given in the previous section but also the strong interaction and dependencies were demonstrated. In the following, more details will be given for the key elements of the multi-disciplinary approach. In order to better understand the dependencies, the works will be presented in dependency order and not in work package groups as in Section II.

A. Sound synthesiser machine

The key requirement towards the Sound Synthesiser Machine is that lay persons, e.g., non-engineers, should be able to use it in such a way that the end result can be used by aircraft manufacturers as an indication, which of the dominant noise sources of an airplane are to be suppressed most of all. This doesn't necessarily mean a simply noise reduction task, as it is also possible, that making a few components a bit louder, one can mask the most annoying noise source without a strong reduction in its level.

It is obvious that making an aircraft quieter will make it less annoying, but it is also well known, that *sound quality* plays an important rule too. The Sound Synthesiser Machine serves exactly this goal, namely to enable subjects to create their own less-annoying-sounding aircraft under the prescription that the more preferred aircraft sound i) is of the same loudness as the original, ii) will be technically feasible at least in the coming 10-20 years.

For most sound design tasks, engineers are employed to invent the best sounding, yet technically feasible sound of a means of transport. Unfortunately those engineers, working for years and decades on sound design, are reacting probably in a different way to aircraft sound, as people living around airports. For the first time a tool has been realised, which allows really lay people, e.g., people who never had anything to do with sound design, to adjust their own preferred aircraft sounds interactively.

The realisation of the sound synthesis machine consists of 3 main steps:

1. C*urrent aircraft flyovers have to be measured* under realistic conditions. E.g., a quiet recording place has to be found in a distance to the runway, where typically houses can already be located. Both take-offs and landings have to be recorded.
2. The recorded aircraft sounds have to be *decomposed into components* (see Fig. 2), which can be seen as the most dominant noise sources of an aircraft. These are for example tonal components of the turbine, the buzz-saw noise, the broadband noise of the airframe, etc. The exact components have been defined by aircraft manufacturers, in a way that they can clearly be distinguished as a sound component (e.g., it is strong enough), but can also be related to a major part of the aircraft (e.g., it is not a mixture of completely different parts of an airplane). This will assure that the level adjustment on the sound components can later directly be translated into the necessary modification of a clearly defined part of an aircraft.

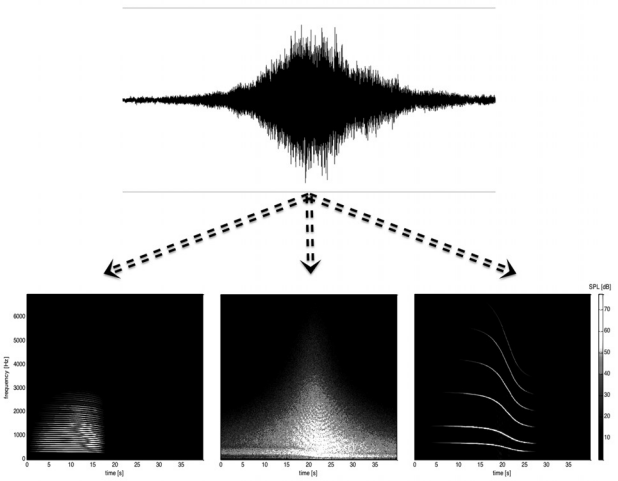


Fig. 2. Decomposition of a recorded aircraft flyover onto source components, like buzz-saw, broadband noise, tonal components, etc. (Top picture: time vs. measured sound pressure signal amplitude, bottom pictures: time vs. spectra of decomposed signals. From left to right: buzz-saw, broadband noise, tones.

3. Finally, a software has to be written, where faders are assigned to the various components, and the subject can adjust the level of each fader such that the mix of the level-adjusted sound components result in a better sounding flyover than the original one. (These new sounds are referred as *target sounds*.) Naturally, the tool has to compensate for the level adjustments of the individual components, making sure this way that the new sound is *perceived exactly as loud* as the original one. As mentioned already, it is of key importance that

the tool can be used very easily. For this reason, not only a very clean and easy graphical user interface has been designed, but also an external controller is applied to control the tool. This makes it possible even for people having less experience with computers to familiarise them with the tool very fast and to be able to realise those sound modifications, which they think to be the best for them.

By realising this way the Sound Synthesiser Machine, examinations can be performed with lay participants in laboratories. In European projects it is of great importance that test are realised in several laboratories all over Europe. As with all such psychometrical examinations, specialists point out the necessity of assurance of as similar as possible conditions at all examination places. Only this assures, that at the end of the examinations, a common statistical analysis can be performed, valid mean values can be computed and cross-cultural differences/similarities can be shown. For this reason, i) headphones were selected for sound reproduction (because using them there is no influence of room acoustics or loudspeaker differences), ii) exactly the same hardware controller is used in all laboratories with the same software (naturally labels are translated in the countries' native languages), iii) the sound reproduction level through headphones is well defined and the same for all places.

In Fig. 3, a participant can be seen working with the Sound Synthesiser Machine.

Fig. 3. Working with the sound synthesis machine

B. *Optimisation of procedures and sequences*

This activity is divided in two optimisation tasks, dealing with single and multiple events, respectively, plus a final task aimed at the formulation of the design criteria.

Single event optimum – e.g. optimised procedures

As a first step, a single-event procedure is analysed. The optimisation objective is the achievement of an optimum noise shape (see Fig. 4) based on one of the target sounds synthesised during an earlier European project, compatible with the aircraft configuration under analysis. During this phase, particular attention must be paid on the compliance of the manoeuvres with specific operational limits in terms of load factor, climb and descend rate, and stall speed. These constraints are taken into account by considering different levels of severity for the operational bounds.

At the first level, the operation conditions are limited by considerations related to flying comfort, in order to avoid sharp manoeuvres and limiting the load factor to values easily tolerable by the passengers.

The second level deals with the constraints imposed by the applicable regulation, which depend on several factors. Here, only the most relevant subset of constraints is applied to the optimisation procedure.

The third level is represented by the operational limits of the specific aircraft under analysis, and is essentially related to airworthiness.

The use of these multilevel constraints allows for a dynamic selection of the criteria to be applied for the identification of the more appropriate procedure. For instance, when dealing with the heavy night traffic related to air courier operations, limitations related to passengers' comfort are not pertinent, and higher load factors (*i.e.*, sharper manoeuvres) can be reached.

The outputs of this optimisation task are noise levels at the certification points, and noise footprint. Once the optimisation process is calibrated on earlier sounds, the updated target sounds provided by the Sound Synthesiser Machine examinations will be used, and the sound-matching criterion (based on the "index of sound similarity") will be extended to the analysis of multiple observation points, in order to produce a map of the matching level of the aircraft noise with the given target.

Multiple event optimal scenario – e.g. optimised sequences

In the present task, the algorithm developed in the single event optimisation task is extended to multiple-events situations, in order to deal with a realistic condition and provide to sound synthesis specialists (see next Section) the appropriate guidelines for the final synthesis of the low

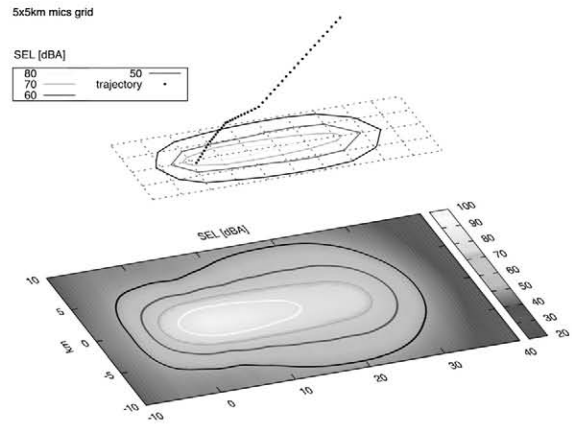


Fig. 4. After optimisation, the footprint of a take-off or landing can b computed and drawn as seen in the figure. Single event optimal procedure result in smaller noise footprints than currently used procedures.

annoyance airport noise scenario. To this aim, the operative framework is defined in terms of number of events, aircraft types, and airport map. The optimisation criteria are specified in accordance with the recommendations arising from the results of the field studies (see Section III/E). In this respect, a crucial aspect is the definition of an appropriate objective function, capable to drive the optimisation process towards optimal solutions consistent

with the outcomes of psychometric research group. Indeed, the identification of the proper objective function is strictly related to the optimisation criteria to be pursued, and thus to the chance of success in the achievement of the desired optimal scenario. In addition, it deeply influences the choice of the simulation models to be included in the optimisation framework.

Another key point to the accomplishment of the present task is the identification of the additional regulation constraints to be included in the optimisation process. In this case, the criteria (optimum noise shape) used during the single event optimisation task must be completed with the restrictions arising from the simultaneous presence of several aircraft in the vicinity of the airport. These restrictions must be provided in terms of event separation time, minimum horizontal distance, minimum vertical distance, and relative speed. In order to keep the computing time within a reasonable limit, only the most relevant limitations to the operations are taken into account.

C. *Synthesis of individual flyovers and sequences*

As mentioned before, the output of the optimisation tasks are flyover paths defined by many points in the 3D space accompanied by a number of aircraft settings parameters (e.g. a large tables). The so-called Airport Noise Climate Synthesiser is a powerful sound synthesis tool that – among other input types – can be fed with these "tables" and is able to synthesise airport noise scenarios for any location in an airport community. Being more precise, the tool uses 5 sets of input data: 1) source component spectra (jet, turbine, fan, etc.), 2) operational parameters (flap settings, speed, engine RPM, etc.), 3) atmospheric noise propagation and ground reflection models, 4) flight path data and 5) airport scenarios (types of aircraft, number of events, time between events, etc.).

This tool bases on a much simpler tool developed in an earlier European Project (SEFA), which was able to synthesise individual flyovers with a highly limited number of aircraft source models. The flyovers produced by the earlier tool were recognisable, but sounded too synthetic. However, the development of that basic version (which can be seen as a beta version for the current one) formed important knowledge about the necessary input data for realistic sounding flyovers.

Several new functionalities are in on-going development in the current approach:

- An interface to the so-called SOPRANO tool (an extensive database of aircraft noise source components), which will serve as a data management tool to support and manage any kind of source component models and data.
- Source component modification capabilities that allow assessing the impact of modification scenarios and technology increments.
- Improved noise propagation models [2], which cover turbulences, wind effects and complex terrain effects.
- The extension of the new tool to support multiple events in real airport scenarios.
- The linkage of the tool to the Virtual Resident (VRes) model (see Section III/F). This allows computing functional noise annoyance maps for airport communities, which is expected as a big improvement over simple L_{DEN} maps.

All software components are developed in an open way and will be able to support additional measurement data, new engine and aircraft technologies, new airport policies and more realistic virtual resident models after the current project finishes. This assures, that such a tool, which is very hard to develop, will not vanish after the end of the project, but can be used and further developed any time.

Without naming all the companies and institutes involved in the actual development, it is worth to mention, that aircraft- and aircraft engine manufacturers, experts in the field noise and vibration, programmers contribute all to the successful development of the tool.

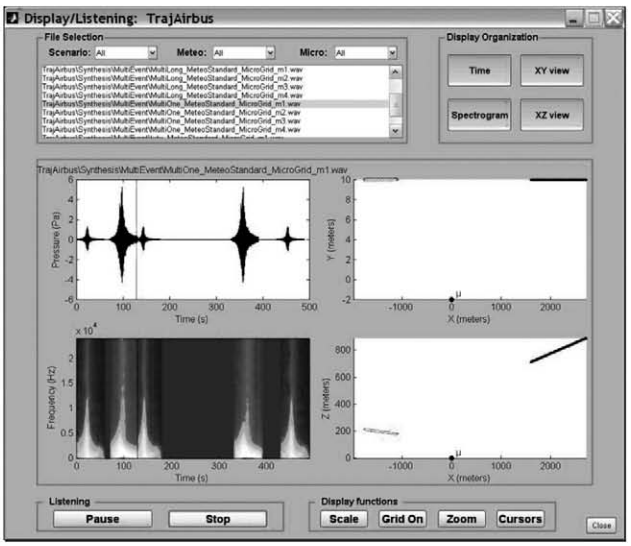


Fig. 5. The Airport Noise Climate Synthesiser takes noise-source components, trajectories, aircraft types, listener position etc. and computes flyover sounds, which can be played back by regular audio software.

In addition to the mono sound synthesis, also a 3D auralisation system is under development to enhance the perception of the synthesised aircraft sounds. This auralisation system will take advantage of the principles and algorithms gained during the development of the Aircraft Climate Noise Synthesiser tool. As a spatial sound reproduction system closely corresponds to reality, psychometric judgments of aircraft sound quality may be substantially more predictive in respect to the Virtual Resident than those that are based on standard methods using headphones. 3D virtual airport scenarios will be auralised using a setup of 8 loudspeakers.

The output of the Airport Noise Climate Synthesiser can be tested in different ways. First of all, the L_{Aeq} contours and the resulting spectrogram can be check. Also by simply listening to the output gives important information to developers about the actual quality at a given stage of the development. However, the final approval can only be done

by psychometric tests asking from participants for quality of the synthesised sounds and their perceptual similarity to measured ones. For this purpose, members of the psychometric group will perform validation tests at the end of the development.

D. Laboratory studies

The results of the optimisation process described in section III/C can be used by the Airport Noise Climate Synthesiser tool to create future aircraft (new engine, new shape, etc.), manoeuvres (new flyover trajectories with the according engine-, flap-, slaps-settings) and airport scenarios (a number of aircraft taking-off and landing). This has the big advantage, that not only *numbers* underlie, that a given change would result in x dB less *loudness*, but also the possibility that one can listen to them. Like real aircraft sounds in the field (e.g. a number of aircraft during a given observation time in listeners home), synthesised sounds can also be tested. They have to be played back through appropriate loudspeakers (e.g. ones with good bass reproduction capabilities) in laboratories arranged like a living room at everybody's home (see Fig. 6). The word "laboratory" means in this case, that the acoustics of the room are well known/controlled.

Fig. 6. Participants taking part in the laboratory studies. In being in home-like surroundings, aircraft flyovers are played back through loudspeakers. Participants do home-like activities like reading, discussing, and in addition also performance tests.

For practical reasons, very long tests – like in the field studies (for details see the following section) – can not be performed, but tests of a duration of several hours can, which are already enough to show at least some effects.

In the present project, participants will perform home-like activities (e.g. reading a newspapers, writing a letter, discussing, resting, etc.). After well-defined time-periods, participants will have to give their opinion, how much they felt them disturbed by the aircraft. During the examination time, participants will also perform a few objective tests (memorisation or computation task, reaction time tests, etc.) so the disturbance can also *measured*, not only asked. To find the most appropriate objective methods, psychologists are also involved in the project.

E. Telephone interviews – field studies

Before going into details on the field studies, the importance of the telephone interviews should be pointed out here. It is well known by today, that aircraft noise annoyance is strongly influenced by many other moderators, than acoustics [1]. Just to mention a few of them: expectation of future aircraft noise, procedural fairness, economic dependency from/ attitudes towards the local airport, social status, environmental consciousness, information recently heard in newspapers, kind and time-frame of activity done at home, financial support by policymakers/the airport for window insulations, etc. All these moderators are not directly related to the air traffic and the noise caused by it, but influence clearly the annoyance. So it makes sense to perform first a large telephone interview survey (in case of COSMA, 1200 persons per airport have been interviewed), as it costs significantly less money, than spending measurement days at participants home, but delivers statistically relevant information about the airport under analysis, which are the key factors to determine noise annoyance.

After the telephone interview, for cost saving measures, a subsample can be selected to take part in the actual field studies. But the question rises, why is it worth to perform another field study, when by today many annoyance studies around airports have been performed already?

The point is, that in these studies, the noise excitation generating the residents' annoyance around airports was usually estimated by integrated measures (e.g. L_{eq}, NNI). These data are calculated for defined periods (day, night) using acoustic data (number and levels of flyovers) of more or less distant noise monitoring stations. Noise load calculations from data of official noise monitoring stations (often kilometres away from residents' position) are quite error-prone procedures. Accordingly, annoyance is just poorly predicted. This becomes evident by the huge variance as shown by numerous field studies and meta-analyses performed in the past. Specific acoustic features, such as the frequency spectra of the individual aircraft noise events, and the temporal distribution over the day were usually disregarded.

To go deeper in understanding aircraft noise annoyance, the present project's method records the noise levels directly

Fig. 7. In the unique approach of COSMA field studies, the "polluting" noise is directly measured outdoors at the location of participants, whereas the indoor noise level is computed from it through out/indoor transfer function measurements. (Note the microphone putted at 4m height on the left hand side of the picture.)

at participants home (e.g. in their garden – see Fig. 7), but also in/outdoor transfer functions are measured. There are also time periods, when the participants are focusing on each individual flyover. During these periods, the indoor time signal is recorded, which allows for complete psychoacoustic analyses. In this unique approach, standard and special psychoacoustic parameters can be correlated to the sound quality evaluation of participants.

In these field studies, whilst outdoor noise levels are continuously logged during 4 days, participants are doing regular activities at home. However, each hour, a specially for these examinations developed software alarms the participant to answer a few questions relating to the activity, its disturbance, location, etc. of the participant during the past hour. This approach – developed by field study specialists – allows for direct correlation of annoyance and noise and – further on – the annoyance with aircraft design and operations.

As not only cultural differences can exist in relationship with aircraft noise but also the various airports are highly different in terms of capacity, operation times, number of runways, etc. three important airports are selected for field studies in the COSMA project:

- London Heathrow LON (one of the largest European airports)
- Cologne/Bonn CGN (high amount of night time traffic)
- Arlanda Airport, Stockholm ARN (important airport of a Nordic country)

F. Virtual Resident

This is a tool that has to simulate the annoyance of people living around airports due to aircraft noise. (More precisely, the tool should simulate a kind of "average" person. – See Fig. 8). It collects most of the information gathered in other activities of the project and uses them to create a highly complex "intelligence". The general workflow on the development and on the prediction algorithm of the VRes is depicted in Fig. 9.

The VRes tool will accept different types of input sounds: single-event and multiple aircraft sounds as used in the laboratory listening examinations, field study recordings and combined laboratory/field audio files. The input sounds/sound scenario can be measured or synthesised. The

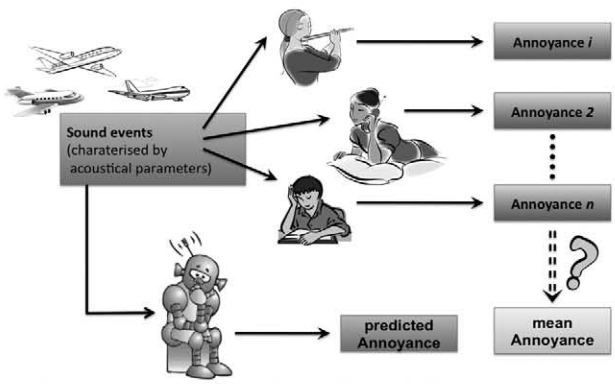


Fig. 8. The challenge of the Virtual Resident. Aircraft noise annoys people during their various activities. One of the major difficulties in the development of the VRes is the specification of a kind of mean annoyance of lot of people during lot of activities. The actual prediction task begins only after.

tool consists of three main modules in serial connection: (1) a preprocessor (parameter extraction) module, (2) the VRes core algorithm and (3) a postprocessor.

In the case of complete sound scenario, the time signature is first decomposed onto single events. Then, a preprocessor module is applied to the input sound data to extract a reduced subset of relevant parameters. This subset of parameters is then passed to the VRes core algorithm. This

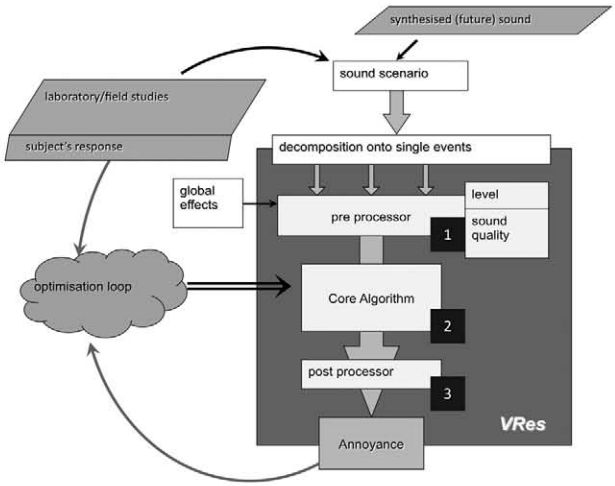


Fig. 9. Workflow of the Virtual Resident.

supports several types of models (neural network model, multi-regression models and categorical & regression tree models), each generating an estimate for annoyance or preference. Finally, the postprocessor selects the most appropriate one or produces a combined estimate.

The VRes tool has a built-in intelligence, obtained from different sources: former field studies, earlier EU projects, sound machine examinations. So it comprises both knowledge and the expertise/know-how of the partners involved. This intelligence is applied to develop both the preprocessor module and the VRes core algorithm models as well.

One of the most challenging tasks in the development of the VRes is the development of the preprocessor. Mathematical algorithms have to be developed to describe the input audio files by a reduced set of parameters. One of the key issues is the definition and selection of those parameters that are most relevant for describing annoyance. Two preprocessor sub-modules are developed focusing on single and multiple events respectively. In case of single events, special acoustic and psycho-acoustic parameters must be computed. For multi-events, the detection of flyovers in the long SPL histories is a big challenge. After successful detection, a few acoustical parameters can be computed for each fly over, and for periods of time averages, distributions, maximal values, etc. The efficient work of the preprocessor is indispensable for the core algorithm, which can handle only a limited number of input parameters for predictions. On the contrary, a time signal or an SPL history log consists of millions/thousands of samples (the values following one after the other).

For prediction problems various algorithms do exist, in the present approach three different types will be realised.

These algorithms must be set up/trained by some measured data. The psychometric examinations described earlier can serve this goal: field/laboratory test's noise records can be used as input for the VRes tool, and its output, the predicted annoyance, can be correlated to human responses. An optimisation process assures the appropriate set up of the internal parameters of the core algorithm. By not using all data for setting up the core algorithms, the remaining data can be used to validate the model.

The last step for the VRes tool is a postprocessor, which i) selects the result of the best core algorithm or combines them, and ii) is able to create an annoyance colour map in cooperation with the Airport Noise Climate Synthesiser.

IV. More information

For further information generally about the COSMA project please refer to [3, 4, 5, 6]. Details about the Sound Synthesiser Machine can be found in [7, 8] about. About annoyance, as a design optimisation criteria can be found in [9]. Further information of field/laboratory examinations can be found in [10, 11, 12]. The Virtual Resident model is described in [13] in more details.

V. Conclusion

The present paper demonstrated a complex approach to further understand and lower communities aircraft noise annoyance. As one could see, this kind of annoyance can not only be handled by simple engineering tools because not only loudness plays an important role, but also other non-acoustical moderators as well. On the other hand, even the acoustical effects are not easily to understand, because aircraft noise annoyance is a long-term reaction. The "combination" of single events to estimate the long-term annoyance is far not obvious.

As these factors are not easy to "measure", the importance of a multi-disciplinary collaboration of researchers and also the broadening the examinations to different places around Europe or the World must be underlined here.

References

[1] R. Guski, "Personal and social variables as co-determinants of noise annoyance", *Noise Health 1999, Volume 1, Issue 33*, p. 45-56, 1999.

[2] F.S.R.P. Cunha; L.M.B.C. Campos, "Acoustic Signal Distortion by Atmospheric Turbulence", in *Proc. of INTER-NOISE 2010*, Lisbon, Portugal, 2010.

[3] M. Bauer, D. Collin, U. Iemma, K. Janssens, F. Márki and U. Müller, "COSMA - Community Oriented Solutions to Minimise Aircraft Noise Annoyance", in *Proc. of INTER-NOISE 2010*, Lisbon, Portugal, 2010.

[4] M. Bauer, D. Collin, U. Müller, K. Janssens, F. Márki, U. Iemma, "COSMA - Progress in Community Orientated Solutions to Minimise Aircraft Noise Annoyance", presented at Aerodays 2011 conference, Madrid, Spain, presentation ID 6E4.

[5] U. Iemma, "X-noise: COSMA project", presented at *Aircraft Noise and Emissions Workshop 2011 (ANEW 2011)*, Rio de Janeiro, Brazil, 2011.

[6] K. Bolin, "COSMA- Community Oriented Solutions to Minimize Aircraft noise- A EU project on sound quality of aircrafts", presented at *International Workshop on Acoustics and Vibration in Egypt - IWAVE 2011*, Cairo, Egypt, 2011.

[7] F. Márki, K. Gulyás, F. Augusztinovicz, R. Bisping, M. Bauer, M. Bellmann, H. Remmers, D. Sabbatini, K. Janssens, "Sound Synthesizer Tool for on-line interactive Sound Quality Analysis of Aircraft Flyover Noise", in *Proc 18th International Congress on Sound and Vibration (ICSV18)*, Rio de Janeiro, Brazil, 2011.

[8] F. Márki, K. Gulyás, F. Augusztinovicz, R. Bisping, M. Bauer, M. Bellmann, H. Remmers, D. Sabbatini, H. Van der Auweraer, K. Janssens, "Sound synthesizer tool for on-line sound quality analysis and target sound design of aircraft flyovers", in *Proc. INTER-NOISE 2011,* Osaka, Japan, 2011, Paper SS61.

[9] U. Iemma, M. Diez, C. Leotardi, "On the use of noise annoyance as a design optimization constraint: the COSMA experience", in *Proc. 18th International Congress on Sound and Vibration (ICSV18)*, Rio de Janeiro, Brazil, 2011, Paper No. 1769.

[10] D. Schreckenberg, R. Schuemer, "The impact of acoustical, operational and non-auditory factors on short-term annoyance due to aircraft noise", in *Proc. INTER-NOISE 2010*, Lisbon, Portugal, 2010, Paper No. 333.

[11] U. Müller, S. Stein, "Community Aircraft Noise Induced Annoyance around Cologne/Bonn Airport - First Results of a Telephone Study", presented at *1st International :envihab Symposium*, Cologne, Germany, 2011.

[12] C. Lavandier, F. Marki, J. Terroir, J. Lambert, P. Champelovier, U. Müller, "Impact of aircraft noise on annoyance and activity disturbance in a laboratory context: pre-test for COSMA project", presented at *ANERS 2011*, Marseille, France, 2011.

[13] L. Kovács, F. Márki, B. Bartha, D. Schreckenberg, "Novel tool for predicting the disturbance of airport residents caused by aircraft noise", in *Proc. Forum Acusticum*, Aalborg, Denmark, 2011, Paper 000554.

Authors

FERENC MARKI obtained his Masters degree in Electrical Engineering in 1998, and his PhD in Engineering and Technology Discipline of Electrical Engineering Sciences (summa cum laude) at the Budapest University of Technology and Economics (BME), Hungary, in 2010. He is associate professor at BME, Department of Telecommunications, where he teaches various courses about audio- and video engineering and acoustics. His research fields are: acoustics (numerical-, room-, psycho- and general), source identification, sound engineering, studio technologies, sound reinforcement. He has more than 15 years computer programming and system administration experience too. Since 2002, he was involved in the following European Projects: TINO, CONVURT, X-NOISE 1/2/3/EV, InMAR, IMAGINE, SEFA and COSMA, where he is workpackage leader.

MICHAEL BAUER, COSMA Co-ordinator, studied physics at the University of Bayreuth and received his doctor's degree on the field of experimental solid state physics in the year 1992. From 1992 to 1998 he was a project leader and consultant for industrial vibroacoustics. In 1998 he entered the acoustics department of Dornier GmbH, Friedrichshafen, as a research and development engineer. He has been working on the Dornier aircrafts Do328Jet exterior noise including flight testing, the Do728 interior noise and turbulent boundary layer noise studies. He was involved in noise certification tests for satellite systems and the European ISS module "Columbus". Since October 2005 he is scientific employee of EADS Innovations Works in Munich, mainly working on propeller and jet noise. Since 2008 he is research team leader for aeroacoustics.

DOMINIQUE COLLIN has worked for 30 years at Snecma, covering various aspects of research and development activities in noise engineering applied to aircraft engines. He is currently Head of Acoustics for the SAFRAN Group, which includes companies such as Snecma, Turbomeca, Messier-Dowty and Aircelle. D. Collin graduated from Université de Technologie de Compiègne in 1978 with a degree in Mechanical Engineering and a masters in Noise and Vibration. After joining Snecma in 1980 as a noise test engineer, he has

been in charge of CFM56 noise engineering and head of the Acoustics Department at Snecma.
Involved since 1991 in ICAO CAEP activities. Dominique Collin is currently Technology Focal Point within the ICAO CAEP Working Group 1 (Noise), in charge of its Technology Task Group. In this capacity, he has co-chaired the CAEP Noise Technology Independent Experts Review performed in 2008.
Since 1998, Dominique Collin is the coordinator of the X-Noise network, an EU funded Coordination Action overlooking European aviation noise research. The X-Noise network which includes all major European industry and research organizations involved in aircraft noise reduction has been instrumental in developing and implementing the current ACARE Strategic Research Agenda (SRA) in the noise area.

UWE MÜLLER obtained his Ph.D. in Physics at the University of Stuttgart-Hohenheim, Germany in 2000. In the same year he joined the German Aerospace Center DLR, Institute of Aerospace Medicine in Cologne. His main competences are in Acoustics and Noise Effects' research. Since 2000 he was involved in respectively responsible for numerous laboratory and field studies about the effects of nocturnal aircraft and freight train noise on residents' sleep using polysomnographical recordings. In two EU-projects he led the workpackages dealing with aircraft noise and sound engineering effects on residents' annoyance.

KARL JANSSENS received his Engineer diploma (1995) and PhD degree (1999) from the Katholieke Universiteit Leuven, Belgium. He joined LMS International in 2001 and works as R&D Project Manager in the Test Department of the company. He has 10 years of experience in sound quality engineering, rotating machinery, noise source identification, transfer path analysis and active noise control.

Prof. **UMBERTO IEMMA**, PhD. Born in Rome, on August 10, 1962. Associate Professors of Aeronautical Structures and Design (Costruzioni e Strutture Aerospaziali) at the Faculty of Engineering of the Roma Tre University. In charge of the courses of "Structural Dynamics" and "Aircraft Design" for the graduate degree program in Aeronautical Engineering, and "Engineering Mechanics" for the undergraduate program in Mechanical Engineering. Responsible of the Laboratory of Industrial Engineering – Section of Aeronautical Structures since 1996. Visiting professor at the Massachusetts Institute of Technology, Cambridge, MA, in Fall 2006. Involved in 10 research projects sponsored by the European Commission in the period 1994-2011. Scientific coordinator of the research unit of the Roma Tre University within the EC projects SEFA, COSMA, OPENAIR. Primary research topics: theoretical/numerical modeling in aerodynamics, aeroacoustics, and aeroelasticity; analysis of the aeroacoustoelastic interaction of shells in motion within a compressible medium; multidisciplinary design optimization of innovative configurations under environmental constraints; development of non-invasive experimental techniques for modal identification of structures; high performance computing using innovative programming techniques; higher-order Boundary Element and Finite Element formulations for aeroacoustics and structural dynamics; fluid-structure interaction in biological flows; theoretical/numerical modeling of acoustic meta-materials for acoustic cloaking. Author of more than 80 scientific papers published on international journals or presented at international conferences with referee.

Interworking and Monitoring of Heterogeneous Network Technologies

Markosz Maliosz, Csaba Simon, Pál Varga

***Abstract*—Wide scope of technologies and research areas has been investigated during the project Together IP, GMPLS, Ethernet Reconsidered – Phase 2 (TIGER2). One of our main contributions was the inter-domain traffic engineering for network load balancing. Inter-domain cooperation at control plane level, forming a „Knowledge Plane" from the various control planes allows the different administrative domains and technology regions to understand and accommodate each other's service and performance requirements. This kind of integrated Traffic Engineering (TE) offers more flexible ways for reacting to traffic changes. Another important contribution was an actual implementation of a traffic analysis equipment that resides in the "Monitor Plane" and reports traffic mix, traffic matrix and further advanced statistics to the Knowledge Plane. The monitoring equipment is an FPGA-based, 10Gbps Ethernet-capable interface card developed for lossless packet capture and advanced traffic analysis.**

***Index Terms*— Traffic Engineering, Knowledge Plane, Traffic Analysis, 10 Gbps Ethernet monitoring**

I. INTRODUCTION

Inter-domain cooperation at control plane level offers the possibility to balance the traffic in a much flexible way compared to the single domain TE methods. We investigate the possibility of cooperation where an Ethernet access network and an IP over WDM (Wavelength Division Multiplexing) core network are interconnected. In our approach a hybrid control plane model is applied where MSTP (Multiple Spanning Tree Protocol) is used as a layer 2-based Ethernet control plane in the access and GMPLS (Generalized MultiProtocol Label Switching) is used in the core. In this network environment the result of the cooperation is redistributing the traffic between the spanning trees of the

aggregation domain. We proposed a joint access-core network optimization based on these cooperating control planes, and investigated our solution by means of simulations.

M. Maliosz and Cs. Simon are with the High-Speed Networks Laboratory, Department of Telecommunications and Media Informatics, Budapest University of Technology and Economics, Hungary. (e-mail: maliosz@tmit.bme.hu, simon@tmit.bme.hu)
P. Varga is with the AITIA International Inc., Hungary. (e-mail: pvarga@tmit.bme.hu)

In order to validate the presumptions about current traffic characteristics both inter-domain and intra-domain, we carried out various measurements at live, operational networks. Beside the fact that these measurements served the modeling phase of the TIGER2 project well, they also showed limitations of current capture and analysis methods. Such limitations included lossless packet capture capabilities at fully loaded 10Gbps Ethernet connections; effective identification of traffic flows carrying peer-to-peer, video streaming or hidden VoIP (traffic mix); and analysis of traffic flows between endpoint clusters (traffic matrix).

II. INTER-DOMAIN COOPERATION OF DIFFERENT CONTROL PLANES FOR TRAFFIC ENGINEERING

A. Selected Network Technologies

Access networks are predominantly Ethernet-based. Ethernet traffic needs to be carried efficiently across an operator infrastructure. The combination of the different technologies: IP, GMPLS and Ethernet yield integrated network architecture in metropolitan carrier-class environments. In such a heterogeneous internetworking environment different data plane technologies and different services at different layers co-exist that need to be harmonized.

From the access network the Ethernet traffic is concentrated at the edge nodes and is forwarded to packet-based transport in the core domain. The trends evolve towards the wide deployment of WDM (Wavelength Division Multiplexing) network devices in the core, which enables the transmission over the established connection-oriented lightpaths in the optical domain.

These lightpaths form a virtual topology over the physical topology that can be reconfigured dynamically in response to traffic changes and/or network planning. The combination of IP directly with WDM results in an efficient assignment of optical network resources to forward IP traffic [1][2].

The versatile GMPLS enables the integrated control of both IP and WDM. Integrated routing and wavelength assignment based on GMPLS is currently the most promising technology, which also delivers effective TE capabilities. The typical routing protocol in such networks is the Constrained Shortest

Path First (CSPF) [3], which enables calculating paths that meet the specific constraints, for example bandwidth requirements [4].

In the above model the lower layer is the 'optical' one, the upper layer is typically the 'electronic' one, capable of performing joint time and space switching. Paths of the lower layer correspond to a single link in the upper layer. Lightpaths are special routes: they arise and terminate in the electronic layer. The upper, electrical layer can perform multiplexing different traffic streams into a single wavelength path (λ-path) or lightpath via simultaneous time and space switching. Similarly it can demultiplex different traffic streams of a single lightpath. Furthermore, it can perform re-multiplexing as well: some of the demands de-multiplexed will be again multiplexed into some other wavelength paths and handled together along it. This is often referred to as traffic grooming [5].

To operate these layers together, we consider the case when both the layers are handled via a distributed control plane to ensure full and joint on-line adaptivity of both of the layers. By using dynamic optical layer, it is possible to create adaptive set of lightpaths that satisfies emerging traffic demands. Those two physical nodes that are connected by a lightpath are seen as adjacent by the upper layer. Multiplexing and demultiplexing the traffic of a lightpath is impossible by applying only optical devices. In these cases lightpaths have to be torn down, their traffic has to be taken up to the electronic layer that increases the number of lightpaths. In addition, the number of applicable opto-electronic converters per node is limited.

B. Cooperation of Control Planes

Typical TE solutions deal with a single domain, only [6][7][8]. Alternatively a joint optimization of traffic over a cascade of core networks has been proposed [9][10], but they consider the same TE algorithm all over the domains.

We assume that the various network segments from the end user until the core edge node (ingress) are merged into one domain. This aggregation-access domain is, or in the near future is expected to be, based on switched layer 2 technologies [11] deploying Multiple Spanning Tree Protocol (MSTP) [12] to steer the traffic to the core. Aggregation and access networks become a L2 switched domain, directly linked to a core network, in which CSPF based TE is used.

Our proposal is to use shared intelligence between control planes, where the core intra-network functions are unchanged and only the inter-network control planes co-operate which enhances the performance. Therefore, we suppose the capability of communicating/cooperating between the control planes of the neighbouring domains.

We investigated the effects of cooperation at control plane level between the different TE mechanisms of the core and access or aggregation domains. The advantage of this cooperation is that it allows much more flexibility in maintaining balanced core network usage by redistributing the access network's traffic among the ingresses. We also investigated the impact of network load optimization on the efficiency of a dual opto-electronic network model [5][13].

It is the task of the cooperating control planes, also called Knowledge Plane, to map the traffic sources among the tree instances of MSTP.

C. Simulations

We designed an aggregation and two core network topologies, a meshed (Figure 1) and a dual ring (Figure 2), that were used for our simulation based investigation.

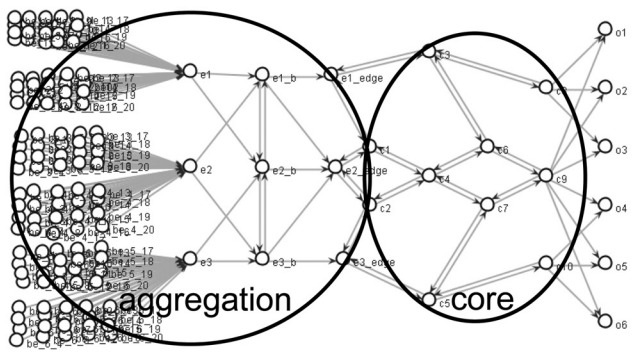


Figure 1 – Aggregation and meshed core network topology

The traffic sources are depicted in Figure 1, the aggregation network conveys the packets to the core network. At the boundary we have three edge nodes. In real life networks the number of edge nodes is also kept as low as possible for reasons of costs. The network has six destination nodes represented by the exit points of the core network on the right side. They are the sinks for all the traffic in the network.

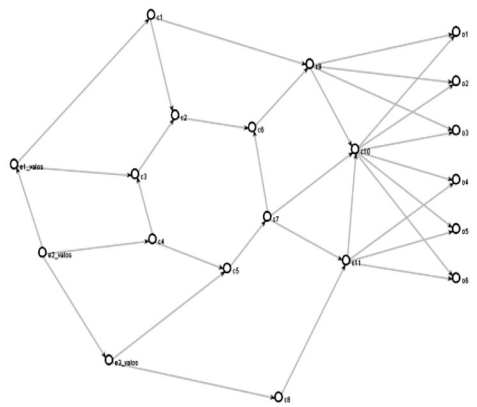


Figure 2 – Dual ring core network topology

The aggregation part of the network can be traversed only in a few hops, with minimal number of alternative routes. The main function of the aggregation domain being the feed of the core network, this is a rational design goal and resembles real life conditions, where nodes are connected to two neighbouring devices, at most. We did not investigate the behaviour (delay, blocking, packet loss, etc.) of the aggregation domain, only determined the input traffic distribution based on the tree topologies of the MSTP for the core domain.

If a TE operation is required in the core network because of a congested link or link failure, etc. using intra domain TE only, the traffic has to be re-distributed only relying on available capacities inside the core. In our proposal, by using the Knowledge Plane, the input traffic distribution outside the core edge routers can be re-arranged too. This means that – from the point of view of the core – we change the input traffic matrix, since the load on the edge nodes will be adjusted.

Let us take the topology presented in Figure 1. In the case when the aggregation domain directs all the traffic to the e1_edge, while e2_edge and e3_edge do not feed any traffic into the core, this is the worst case situation to overload the core and corresponds to the situation when only the tree rooted in e1_edge is used to collect the traffic in the aggregation domain. If we use each of the trees in the aggregation domain to forward the same amount of traffic, then the aggregation domain distributes the traffic evenly among the three ingresses. In this case all regions of the core will be evenly loaded.

The task of the Knowledge Plane is to map the traffic sources among the trees. In our simulations we used small individual flow throughputs. Each tree is collecting such individual demands and the sum of these represents the traffic load at the edges. Practically the granularity of the traffic is small enough to allow us to finely balance the load. In what follows we will use the term load balancing as the operation of load redistribution in the aggregation domain as described above. The goal of load balancing will be to decongest a certain area of the core network with a minimal redistribution of the original load.

Apart from investigating the efficient network capacity usage and balanced load of the core domain, we also investigated the possibility to minimize the operations in the electronic layer and the usage of longer optical paths. These last two parameters are characteristics of the dual opto-electronic models.

D. Results

We assumed that the traffic matrix is known in the core network, and the paths in the core are computed using the CSPF protocol. We had foreground and background traffic which enter the core at the edge nodes and sink on the most right-hand side destination nodes. The link capacities and the topology determine the throughput of the core. We determined the load range where the core network becomes congested (500-800 Mbps traffic volumes).

In our investigations we used only one edge node (e2_edge) as the starting point to feed the traffic of the aggregation network into the core. This path is called the main branch.

If the traffic load is high enough, only part of the traffic can be served. If we apply our solution to this situation, then some part of the traffic will be shifted to the other two edges, e1_edge and e3_edge. The paths that follow the flows entering on these two edges are called secondary branches.

We use the background traffic to "fill" the network up to the point where congestion might start to develop. We sent background traffic on the main branch then we started to add new traffic demands until no more traffic could be carried in the network, which was set differently from case to case. In this range are the interesting scenarios i.e., when the main branch was overloaded, but with the use of secondary branches we still could serve all the demands.

Within each scenario –that is for different overall traffic volume– we have simulated several sub-cases, where the load of the main branch was gradually re-distributed among the secondary branches. At first we let all the traffic to flow through the main branch. Then 30% of the total traffic was forwarded to edges e1_edge and e3_edge (15% on each of them). From there on we stepwise directed more and more traffic towards to the secondary branches (each time cutting 5% more from the main branch). In each scenario we increased the re-distribution ratio until we could serve all the traffic through the core.

From the aggregation network side we calculated all the spanning trees that can potentially be used in our scenarios, that is, all the trees that are rooted in one of the three edges and the traffic sources are their leaves. The traffic distribution on the edge nodes is realized by sharing the traffic among these spanning trees in the aggregation network.

Load Balancing in the Core Network

Figure 3 presents the ratio of successfully served traffic demands in the meshed core. We achieved similar results for the dual ring topology too. It can be seen that increasing the redistribution ratio linearly increases the rate of served demands, until reaching 100%, and also the ratio of the traffic volume that must be redirected to achieve 100% is increasing with the load linearly. These results confirm that if we redistribute the traffic before it hits the core edges, we can balance the core load thus it is a viable mechanism to actively increase the efficiency of the core traffic engineering process.

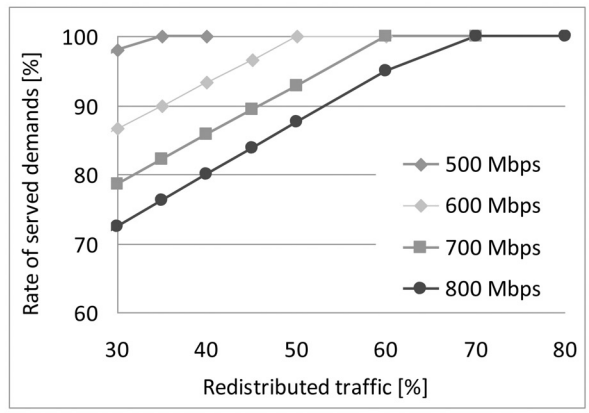


Figure 3 – The successfully served demands as the function of traffic re-distribution

Effects on Opto-Electric Layers

We evaluated the efficiency of the opto-electric transport core network while using traffic redistribution at edge nodes. First let us examine the results in the meshed core. We investigated the number of established lightpaths.

If we compare figures 3 and 4 we can see that as the rate of successfully served traffic demands is rising, but is still below 100%, the number of lightpaths is increasing. This is due to the fact that more and more individual flows are in the network and these are following new (alternative) routes. Thus, the increase of this parameter is not a consequence of the decreasing efficiency but the growth of the core utilization.

This trend is reversing though, if we are looking at the case when we keep redistributing the traffic even after all the traffic reaches its destination. To highlight these results they are encircled in Figure 4 and 5. As we can see in these cases the number of paths is decreasing.

If the primary goal is the minimization of the operations in the electrical layer, the best option is the use of the distributed traffic. The drawback of this solution is that we have to use the alternative branches.

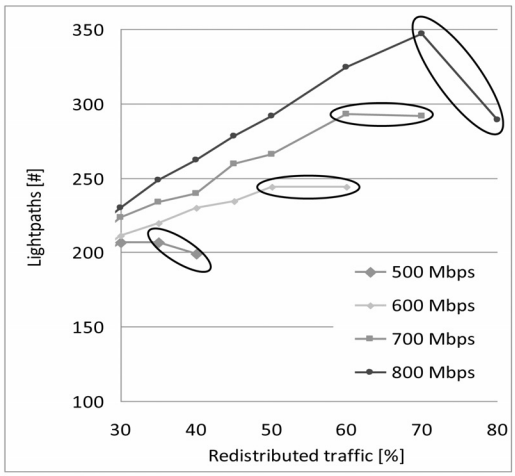


Figure 4 – Number of lightpaths in meshed core

Figure 5 presents the number of opto-electronic conversions done in the core (we encircled the values that yielded 100% success rate). We have plotted in the same graph the results for both the meshed core and dual ring core. These conversions can happen only in the nodes that make a grooming operation and multiple conversions may happen in such a node. The trend observed for the number of the lightpaths is valid also here, for both core topologies.

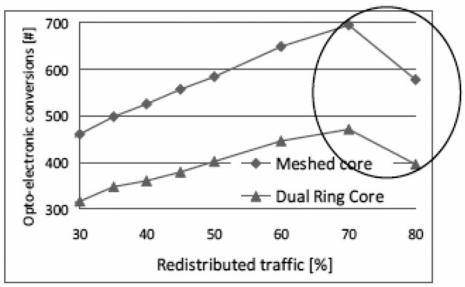


Figure 5 – Number of opto-electric conversions

III. ADVANCES IN THE MONITOR PLANE FOR 10GBPS ETHERNET

Traffic analysis of network segments is an effective method to reveal suboptimal configuration, hidden faults and security threats. If the analysis results are promptly acted upon, improvements in service quality are experienced by both the network operator and the end-user. The concept of the Knowledge Plane (KPlane), and later the Monitor Plane (MPlane) has been introduced to support Autonomous Networking goals. The tasks of processing the network element-, service-, and traffic-information belong to the MPlane. It feeds the KPlane with valuable information, based on which configuration changes are actuated.

The main source of "knowledge" is the actual traffic of the Control and Data Planes. Although some traffic characteristics can be gathered by analyzing the Control Plane messages, many important applications – such as Peer-to-Peer (P2P) downloads, Video Streaming, or interactive voice – hide their control messages, hence their identification is only possible through Deep Packet Inspection (DPI) of the traversed traffic. Traffic mix and traffic matrix analysis results are of major interest in the decision making process at the KPlane. The aim of Traffic Mix analysis is to determine the distribution of volumes for services and applications utilizing the network. Similarly, Traffic Matrix analysis provides results about traffic volumes – and is possible, further characteristics – broken down by route directions.

We follow the functionally split architecture of the Knowledge Plane suggested in [14] (see Figure 6), and further elaborate the functions and requirements of the Monitor Plane. This function is crystallized at the original definition of autonomous networks, in [15], defining the foursome of "Monitor-Analyze-Plan-Execute" (MAPE) functions. The core function of the MPlane is to provide complete and detailed view of the network and its services. Probes at every element (access nodes, routers, switches, content servers, links, etc.) monitor the element status as well as traffic parameters.

Although built-in probe modules seem convenient for reporting - since they are already part of a functional node in the network -, passive probing is more desirable. Active network elements (such as routers or switches) keep their processing priorities to their main job, occasionally leaving the Knowledge Base without information. These occasions of degradation in the status reporting function happen at the worst time from the KPlane's point-of-view – for practical reasons. It gets degraded at the time when the element is getting overloaded. Coincidentally, such detailed reports of overloading would be the most beneficial for the KPlane. This is why passive probing is more desirable to gather information on these elements [16].

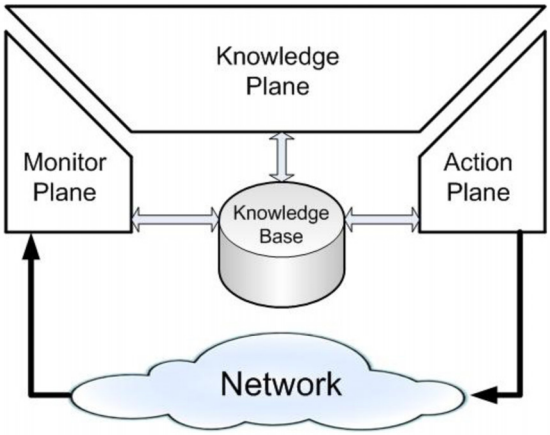


Figure 6 – The Knowledge Plane concept and its functional splitting into three planes

After capturing the raw data, the probes insert processed, grouped, and filtered traffic information into the Knowledge Base. Both packet- and flow-level analysis reveal important characteristics on Quality of Service (through statistics of losses, delays, and jitters in the traffic), routing specialties, network structure changes, violations of the SLS (Service-Level Specification), and if correlated with traffic identification results, even media QoE (Quality of Experience) can be estimated.

During the TIGER2 project we have elaborated the requiments against the Monitor Plane in 10 Gbps Ethernet environment. We also suggested and later implemented a distributed monitoring architecture, in which SGA10GD assures the lossless packet capture and the SGA-GEM (Signaling Generators and Analyzers - Gigabit Ethernet Monitoring) analysis system calculates the traffic statistics on-the-fly, in order to feed the KPlane with input. During TIGER2 we focused on the MPlane implementation.

The main result from the development side is that the SGA10GD network interface card has been planned, designed, developed, implemented and tested during the project. Moreover, we were able to run measurement campaign with this card in real operator's live links - during the short period of the project.

Figure 7 depicts the internal structure of the SGA10GD interface card, whereas Figure 8 gives a picture about its actual physical looks.

The device has the following main components:

- The PCI Express endpoint connector sourced from a 100Mhz external clock allows an FPGA design to support x1, x4 and x8 gigabit lanes to communicate with the host at the speed of 2.5 Gbps of each,

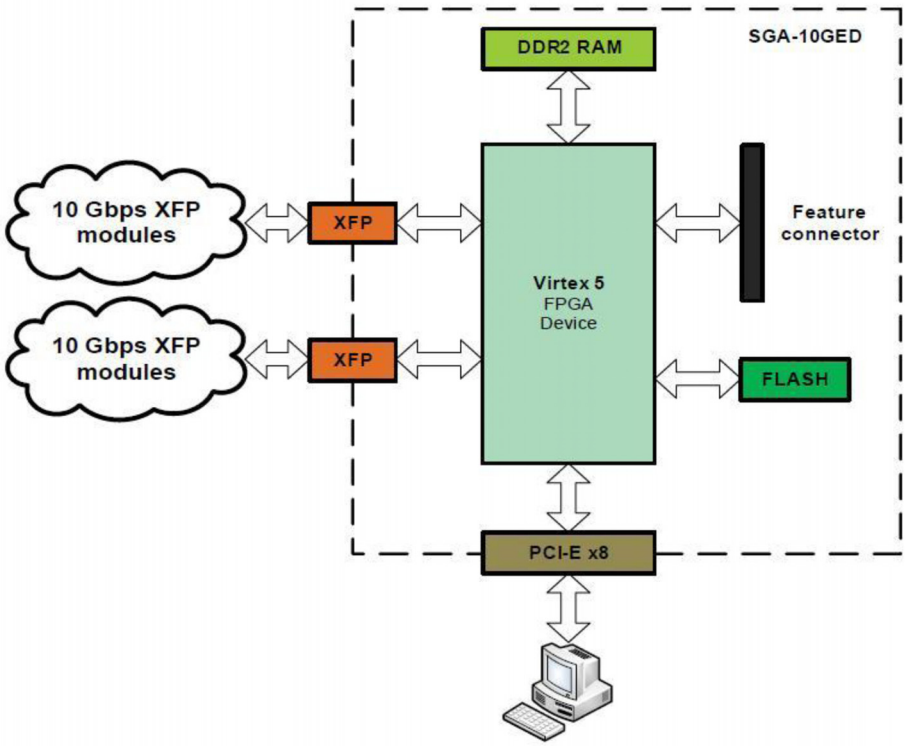


Figure 7 – The environment and the main building blocks of the SGA10GD device

- Dual XFPs for 10Gbps Ethernet (works from 156.25Mhz VCXO clock source): the board has two XFP module cages that support user-installed XFP modules for Gigabit Ethernet (10Gbps) interfaces,
- DDR2 SODIMM RAM: the board contains a 200-pin, small-outline dual in-line memory module (SODIMM) receptacle that supports installation of DDR2 SDRAM SODIMMs of 128MB, 256MB, or 512 MB,
- 40 pin BERG type Feature Connector,
- Xilinx PROM FLASH Platform to reconfigure FPGA.

Figure 8 – Physical setup for the SGA10GD interface card

Hardware components alone does not automatically guarantee useful applications, but it can assure the products future market success. Therefore we considered the following main guidelines to meet current and near-future application-requirements:

- 64 bit Timestamp with 4/8 nsec resolution
- lossless packet capture limited only by host PC's speed and resources
- header-only capture: configurable protocol layer depth decoded by hardware on the fly
- fully PCAP/WINPCAP compliant interface parameterized line speed capable packet/flow generator for active measurements

After the successful lab-tests the SGA10GD card and its analysis environment were taken outside to the real world. There has been three different experimentations carried out during the 2010 summer period: two at different operators' sites in Hungary, and one at BME campus. All cases provided real-life circumstances for the device.

The aim of the experimental measurements at operators were twofold: first, to evaluate the performance of the device and to prove its lossless feature, and second, to provide valuable information for the operators about their traffic at the network segment.

Although detailed analysis results on the operator-specific measurements and analysis cannot be disclosed, some facts about the experiment must be noted:

- Measurements were carried out in both *full capture* and in *header capture* modes,
- *No frame loss* were noted during the measurements,
- Measurements were made for traffic carried through MPLS: the capture device detected and handled it properly,
- Some part of the traffic was tunneled through L2TP (Layer 2 Tunneling Protocol); the analysis environment was able to detect it and create the measurement analysis based on the data inside the tunnel (and not based on tunnel addresses),
- Traffic flowing through both MPLS and L2TP was also handled properly,
- *Traffic mix* and *traffic matrix* analysis were carried out and the results were handled to the expert teams. We successfully detected IPTV traffic, P2P downloads, Skype traffic and many other applications,
- *Analysis on Top-N users* were requested by the operators and the results met their expectations.

Besides providing the analysis results through a standard SQL database, the traffic characteristics, mix and matrix analysis reports are made visible through a Web-based graphical user interface. An example of traffic volume visualization is depicted by Figure 9.

Due to the successful trial measurement campaigns, one of the operators already utilize the capabilities of the SGA-10GD interface card. The equipment has got integrated into their standard network and service monitoring system and currently provide raw measurement data as well as analysis results in the monitored network segment.

TIGER2 results lead to further developments in the domain of traffic analysis of high speed networks. The knowledge gathered through researching the advances of the MPlane and KPlane, as well as the development of the FPGA-based, 10Gbps Ethernet-capable card for lossless packet capture lead to the development of a complex networking device, the C-board is a versatile programmable platform capable of handling 10Gbps Ethernet traffic. It provides a base platform for various packet processing applications such as switching, routing filtering, monitoring, etc. Its modular structure allows its extension with processing cards to increase its applications with high-speed software processing as well [17].

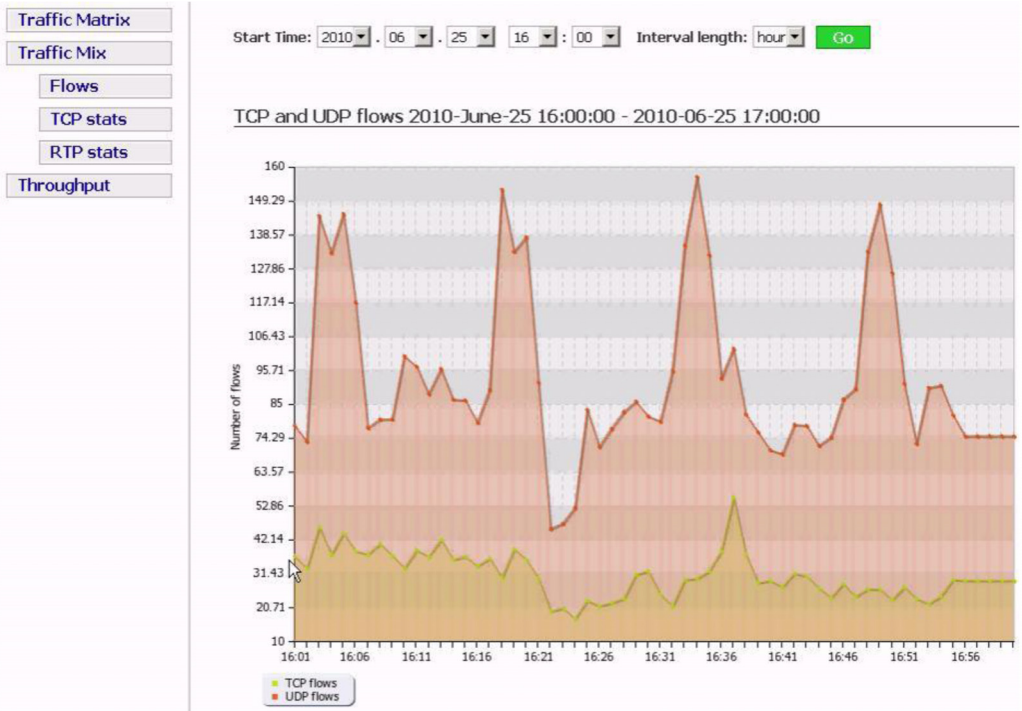


Figure 9 – Visualization example for the number of parallel transport level flows, analyzed by the MPlane

IV. CONCLUSION

With an adequate traffic management solution the performance of the core network can be improved. We have shown that if congestion occurs in the core, we can eliminate the congestion just with a proper coordination between the control planes of the aggregation and core domains, redistributing the traffic prior entering. This solution increases the ratio of successfully served traffic demands, increasing the utilization of the core. The traffic redistribution at the aggregation has positive effects even if there is no congestion in the network, because in such cases it increases the efficiency of the opto-electronic transport layer.

The FPGA-based SGA10GD interface card and the corresponding firmware and software codes were not be reality without TIGER2. The cutting-edge device can now be put into operation for various networking tasks including 10Gbps Ethernet traffic measurements, firewalls, and other programmable nodes. Its lossless capture capability and its ability to provide a base for Monitoring Plane applications such as traffic mix and traffic matrix analysis have been proven through various laboratory- and field-tests. The Knowledge Plane for larger networks with full load may require greater processing capabilities, and a more scalable Monitoring Plane.

ACKNOWLEDGMENT

This work has been partially funded in the framework of the CELTIC TIGER2 project (CP5-024) as part of the EUREKA cluster program.

Parts of the research leading to these results has also received funding from the ARTEMIS Joint Undertaking under grant agreement n° 100029 and from the Hungarian National Office for Research and Technology (NKTH).

The authors would like to thank the contribution of Gyorgy Horvath (BME-TMIT), Laszlo Kovacs (AITIA) and Gabor Krodi (AITIA).

REFERENCES

[1] Kevin H. Liu, "IP Over WDM", John Wiley & Sons Inc., ISBN: 9780470844175m 2002.

[2] B. Mukherjee, "Optical WDM Networks", *Optical Networks Series*, Springer, ISBN: 978-0-387-29055-3, 2006.

[3] M. Ziegelmann, “Constrained Shortest Path and Related Problems. Constrained Network Optimization.” VDM Verlag Dr. Müller. ISBN 978-3-8364-4633-4. December 2007

[4] Y. Lee and B. Mukherjee, "Traffic engineering in next-generation optical networks", In: IEEE Communications Surveys and Tutorials, Vol. 6, Nr. 1-4 (2004), p. 16-33.

[5] T. Cinkler, “Traffic- and λ-Grooming”, *IEEE Network*, pp. 16-21, March/April, Vol. 17, No. 2., 2003.

[6] E. Osbourne, A. Simha, “Traffic Engineering with MPLS”, Cisco Press, Indianapolis, ISBN 978-1-58705-031-2, 2003.

[7] B. Fortz, J. Rexford, and M. Thorup, "Traffic engineering with traditional IP routing protocols," *IEEE Communications Magazine*, vol. 40, no. 10, pp. 118-124, 2002.

[8] S. Dasgupta, J. Cavalcante de Oliveira, J.-P. Vasseur, “Dynamic traffic engineering for mixed traffic on international networks: Simulation and analysis on real network and traffic scenarios”, *Computer Networks* 52(11), pp. 2237-2258, 2008.

[9] R. Casellas, R. Martvnez, R. Mupoz, S. Gunreben, “Enhanced Backwards Recursive Path Computation for Multi-area Wavelength Switched Optical Networks Under Wavelength Continuity Constraint”, *Journal of Optical Communications and Networking (JOCN)*, vol. 1, No. 2 pp. A180-A193, ISSN: 1943-062, Jul. 2009.

[10] K-H. Ho et al, "Inter-autonomous system provisioning for end-to-end bandwidth guarantees", *Comp. Commun.*, v.30 n.18, p.3757-3777, Dec. 2007.
[11] L. Fang. N. Bitar, R. Zhang, M. Taylor, "The Evolution of Carrier Ethernet Services: Requirements and Deployment Case Studies," IEEE Commun. Mag., pp. 69–76, March 2008
[12] L. F. Caro, D. Papadimitriou, J. L. Marzo. "A performance analysis of carrier Ethernet schemes based on Multiple Spanning Trees", *VIII Workshop in G/MPLS networks*, Girona, Jun. 2009.
[13] R. Sabella, H. Zhang, eds.: "Traffic Engineering in Optical Networks", *IEEE Network*, March/April, Vol.17, No.2, 2003.
[14] Latre, S., Simoens, P., Vleeschauwer, B.D., Van de Meerssche, W., De Truck, F., Dhoedt, B., Demeester, P., Van Den Berghe, S., Gilon, E., "Design for a Generic Knowledge Base for Autonomic QoE Optimization in Multimedia Access Networks", In Proceedings of 2nd IEEE Workshop on Autonomic Communications and Network Management, Salvador, Brazil, April 2008.
[15] IBM, "Architectural Blueprint for Autonomic Computing", 2003.
[16] P. Varga and L. Gulyas. Traffic analysis methods to support decisions at the knowledge plane. Infocommunications Journal, 65,10, 2010.
[17] P. Varga, I. Moldovan, D. Horvath, and S. Plosz. A low power, programmable network platform and development environment. In Advances of Network- Embedded Management and Applications, Chapter 2, pp.19-36. Springer, 2010.

Csaba Simon is a research engineer at the Department of Telecommunication and Media Informatics of the Budapest University of Technology and Economics (BME). His research interests are network architectures and design, QoS of IP networks and network management systems. He participated in numerous national and international projects in the fields of network management systems, multimedia and optical network services. He is a member of Scientific Association for Infocommunications, Hungary (HTE).

Markosz Maliosz received his MSc (1998) and PhD (2006) degrees in informatics in the field of infocommunication systems at Budapest University of Technology and Economics (BME). He is an assistant professor in the High-Speed Networks Laboratory at the Department of Telecommunication and Media Informatics, BME. His main research areas are network architectures and design, optimization techniques and traffic engineering. He participated in numerous national and international projects in the fields of network resource management, multimedia and optical network services. He is a member of Scientific Association for Infocommunications, Hungary (HTE).

Pal Varga is a subcontracting project manager at AITIA International Inc. Besides, he is an assistant professor at Budapest University of Technology and Economics, Hungary, where he got his M.Sc. and Ph.D. degrees from. He previously worked for Ericsson Hungary (software design engineer for AXE10 subscriber services) and Tecnomen Ireland (system architect for Tecnomen's Intelligent Network solution). His main research interests are switching and routing, service and network management, network performance measurements, fault localization, traffic classification, e2e QoS and SLA issues. He has been involved in various European projects, playing both technical and project leading roles.

Components for Integrated Traffic Management: The MEVICO Approach*

László Bokor†, Zoltán Faigl†, Jochen Eisl‡, Gerd Windisch§

***Abstract*— Mobile Internet has recently turned into reality for great masses of users, which implies an immense traffic explosion in the packet switched wireless domain up the next few years. As the demands on the infrastructure increase tremendously, mobile network operators will recognize that, if they intend to deliver Internet access by satisfying the customers' expectations, managing traffic inside their network and controlling the affected network resources will require a lot more efficient and complete solution than ever before. In this paper we introduce new, innovative concepts and schemes for traffic management, which have not yet been deployed within commercial mobile networks, and which are subject of our work within the CELTIC-Plus MEVICO project. All the devised traffic management techniques are grouped into specific building blocks to help the reader to understand the complexity and possible dependencies among the existing proposals. As a conclusion, an outlook on the integrated MEVICO traffic management architecture that incorporates the presented mechanisms is also given.**

***Index Terms*— micro- and macroscopic traffic management, improved resource selection and caching, application supported traffic management, steering user behavior.**

I. INTRODUCTION

Current forecasts and researches (e.g., [1], [2], [3]) show that an inevitable mobile traffic evolution is foreseen thanks to the following main factors: growth of the mobile subscriptions, evolution of mobile networks, devices, applications and services, and significant increase potential in the number of devices resulted by the surge of novel subscriptions prognosticated for Machine-to-Machine communications [4]. Existing wireless telecommunication infrastructures are not prepared to handle such an expansion. As mobile and wireless communication networks move toward broadband converged networks and applications, the demands on the infrastructure grow exponentially [5].. High capacity LTE/LTE-A networks will follow the same path as wireline networks in the past, and will thus become quickly dominated by Content Delivery Network (CDN) and peer-to-peer (P2P) traffic. The high amount of wireless bandwidth available makes it possible to provide capacities typically consumed by PCs on broadband connections. On the other hand, it can be recognized that wired segments of mobile operator networks remain static regarding available capacity and throughput. The latter increases the need of smart and integrated traffic management (TM) solutions for backbone networks and for the terminal side to be able to run multimedia applications efficiently.

It will become essential that the network must be aware of the traffic type of each application and enforce possibly individual TM and control (i.e., priority, routing, bandwidth, etc.) required for ensuring improved QoS/QoE for every user. Ensuring that mobile networks are application-aware, can help to achieve flexible adaptation to any new application and traffic pattern emerging in the future. Operators need to install effective tools to manage traffic using QoS policies, bandwidth allocation schemes, prioritized access and admission control, traffic shaping and rate control, and flow based processing. Only such advanced and active TM will guarantee that operators can provide cost-effective data transfer with real-time speech and video on heterogeneous accesses.

Traffic control forms part of the management process of operational networks with close relations to network planning and resource deployment. TM covers all measures to dynamically control and optimize traffic flows in a network domain or in a global view of the interconnected Internet, aiming at ensuring a maximum throughput and sufficient QoS for the users. Therefore TM includes concepts for dimensioning, admission control, differentiation of services and failure resilience that should guarantee a well balanced load level for good performance in normal operation and maintain availability of important services for a set of main failure scenarios.

In this paper we introduce our preliminary results on traffic management for future mobile Internet architectures in the context of the CELTIC-Plus MEVICO (Mobile Networks Evolution for Individual Communications Experience) project [6] in order to underline the basics for subsequent concept and solution development tasks. To achieve this we first summarize the technical approach of project MEVICO in Section 2. Then in Section 3 we derive the general building blocks of advanced traffic management aiming to improve resource usage and QoE for users in the Evolved Packet System (EPS). We detail the building blocks and give example schemes for each of the blocks in Sections 4, 5, 6, 7, 8 and 9. Section 10 provides the initial outlook on how these traffic management mechanisms may interact with each other in

* This work has been performed in the framework of CELTIC project CP7-011 MEVICO and also supported by the MEVICO.HU project of the Hungarian National Development Agency (EUREKA Hu 08-1-2009-0043).

† Budapest University of Technology and Economics, Mobile Innovation Centre, Budapest, H-1111, Bertalan Lajos u. 2, Hungary. E-mail: bokorl@hit.bme.hu, zfaigl@mik.bme.hu, Corresponding author: László Bokor

‡ Nokia Siemens Networks GmbH&COKG, St.-Martin-Str.76, 81541 Munich, Germany, E-mail: jochen.eisl@nsn.com

§ Chemnitz University of Technology, Reichenhainer Str. 70, 09126 Chemnitz, Germany, E-mail: gerd.windisch@etit.tu-chemnitz.de

foreseen future scenarios. We summarize our findings so far and conclude our paper in Section 11.

II. THE CELTIC-PLUS MEVICO PROJECT

The research project MEVICO [6] investigates aspects of the 3GPP LTE-mobile broadband network for its evolution in the near/mid-term in 2011-2014 and beyond. The goal is to contribute to the technical drive and leadership of the Evolved Packet Core (EPC) network of the 3GPP, and thus support the European industry to maintain and extend its strong technical and market position in the mobile networks market. The project follows an end-to-end (E2E) system approach on evolution of the EPC. The focus is on the connectivity layers of the system, for example on the part of the future LTE network which provides the efficient packet transport and mobility support for the applications and end-user services accessed over the LTE and LTE-Advanced radio systems. The technical research of the project covers relevant topics in the areas of network architecture, mobility and routing, packet transport, traffic management, network management and engineering, and techno-economic aspects.

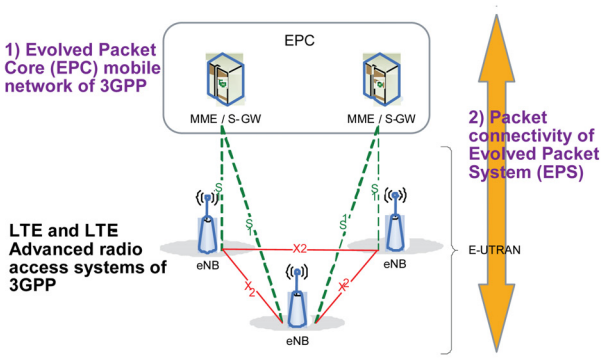


Fig. 1. Focus of MEVICO on the mobile packet core network and packet system of 3GPP

The project does not address the radio interface aspects, but rather tries to enhance the network architecture for small cell structures, higher bit rates and higher capacity. Nevertheless, the peculiarities and limitations of the radio portions are reflected into the core network and those impacts are therefore subjects of analysis. For this, new network technologies and concepts will be studied to apply them to the mobile packet core to further evolve the EPC for the future challenges (Figure 1). Examples of such opportunities are wide-scale availability of optical transport, packet transport (IP, Ethernet) throughout the mobile network, and self-organizing networks (SON) for the network management. The increasing number of mobile users and their consumption of mobile data services result in increasing capacity requirements for the mobile packet core network. The expected growth of data traffic is to be addressed in the research throughout the system. For this, technical concepts for further optimization of the system will be considered. A driver in this is the cost efficiency in operational (OPEX) and capital (CAPEX) expenditures for the case when the operator revenues are not growing in proportion with the traffic.

The research and innovation work in MEVICO project is mapped into five technical Work Packages (WPs, see Figure 2). WP1 (System Architecture) deals with collecting the system level requirements and designing the core system architecture for the next generation mobile systems. WP2 (Mobility and Routing) is responsible for the mobility related researches in LTE/LTE-A, where the main challenges are coming from the novel radio technologies and network topologies. WP3 (Packet Transport) focuses on new strategies and concepts in LTE backhauling, which arise e.g., from the strong needs for increased capacity and better QoS. WP4 (Traffic Management) first collects functional, architectural and operational requirements for the traffic management subsystem, and then designs and evaluates an advanced and integrated traffic management framework for the future broadband wireless telecommunication networks. WP5 (Network Management and Engineering) identifies the key issues and proposes self organizing solutions to them in the area of network management and engineering of the next generation networks. WP6 (Techno-economics and Migration) deals with the techno-economical evaluation of the different aspects of the MEVICO architecture, and also outlines the potential migration path towards that future scheme. In order to better synchronize the work between different Work Packages, vertical cross-WP themes have been established for Architecture, Standardization, and Validation topics.

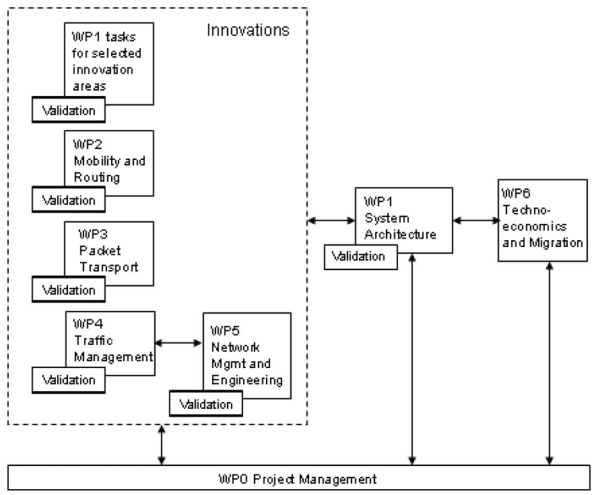


Fig. 2. Structure of Work Packages in MEVICO

Within the above framework of MEVICO, the Traffic Management work package identified the following general challenges to be tackled by the components of an advanced TM system in future mobile architecture:

- Satisfy user experience with minimum of infrastructure resources and still be flexible to handle the possible large variation of traffic patterns over time.
- Initiate handovers of sessions and/or flows not only based on signal degradation, costs, etc. but also based on a possible threat of congestion or any other threat on the QoS/QoE conditions.
- Provide QoS differentiation based on both applications

and user profiles and ensure an appropriate scheme of user and application prioritization and differentiation which is not limited to forwarding behavior but may consider access control as well.
- Split and manage connections (e.g., TCP sessions) over multiple flows inside the network.
- Optimize P2P and massive multimedia transmissions over the network.
- Solve the problems of existing combinations of link layer ARQ and TCP.Unnecessary TCP retransmission causes unwanted traffic through the network and reduces application throughput and response times.
- Optimal design and efficient management of Content Delivery Networks in an operator's infrastructure (e.g., identify suitable locations for caching, select suitable locations for content, detect unfavorable resource usage, redirect requesting node to alternative resource, etc.).
- Implement efficient offloading techniques, access network/core network elements (re)selection schemes in order to effectively distribute users' data traffic through localized wireless access points (femtocells or WLAN) and to locate service gateways (breakout points) near to those access points (aiming to avoid non-optimal routing and overloading of the network elements).
- Supply switch on/off schemes of networking equipments with traffic management aware decision algorithms.
- Anticipate applying an intelligent planning process for extending the available resources (i.e., design optimal or near-optimal capacity extension procedures which are able to cope with the enormous traffic volume evolution).
- Enable fast re-active mechanisms based on detection of application and network layer events to accomplish rate adaptation for multimedia streaming application and synchronization with resource management in EPS networks.

A Traffic Management framework handling the above challenges requires a very wide scale of different techniques, mechanisms and protocols. The MEVICO project does not try to fully cover all the above problems but to show how solutions for certain questions can be integrated in an efficient and comprehensive way into the overall MEVICO system architecture.

III. Traffic Management Building Blocks

Modern traffic management possesses a very rich and diverse toolset including methods and schemes for e.g., dimensioning, admission control, service and user differentiation, failure resilience, etc., but lacks a generic model for common understanding and prevailing basis of developments. This section describes the traffic management building blocks we derived in MEVICO to cover the identified challenges and to provide a universal scheme and a comprehensive overview of the potential mechanisms to improve user's QoS/QoE and to enable efficient usage of infrastructure and IT resources. For the latter there is a benefit for other stake holders in the (mobile) communication business, such as communication service providers and mobile network operators (MNO), content providers and content distribution network (CDN) providers. We have identified six different categories, which can be used to assign the various techniques and aspects of an advanced traffic management system. Figure 3 displays these principal building blocks with some relevant examples. The idea behind the division into these building blocks is on one hand the time dimension. The first four blocks act in real-time on flows, whereas the last two, namely Steering User Behavior and Deployment of New Network Resources are done much less frequently and they are more of strategic decisions. Other than that, the mechanisms are also divided into blocks in the sense of whether they affect a single flow or they are more global in terms of better utilization of network resources. Moreover, there are three blocks, which may be correlated with each other (like lower layer functions providing services to higher layer functions in a communication stack), namely, microscopic traffic management (MicTM), macroscopic traffic management (MacTM) and improved resource selection and caching (IRSC).

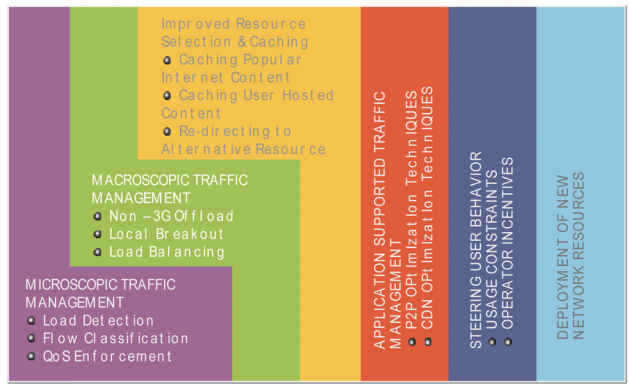


Fig. 3. Traffic management building blocks

MicTM is associated with all mechanisms with the primary objective to improve performance of individual flows based on application type, user profile and other policy related information. MacTM includes all mechanisms with the primary objective to improve efficient usage of network resources. Parameters for optimization in the latter case describe traffic patterns without detailed knowledge of individual flow attributes. Sample mechanisms for MacTM are (re)selection of core network elements and IP Flow Mobility (IFOM). Some mechanisms for MicTM are support of multipath flows (e.g., Multipath TCP, MPTCP), real-time and QoS differentiation based on applications and offline traffic analysis techniques which try to classify network traffic into applications in a larger grade and non real-time so that the operator can get to see big picture and use it to configure and fine-tune Deep Packet Inspection (DPI) tools. The mechanisms associated to IRSC address the selection of resources in distributed data management systems (P2P, CDN, caching). This building block may rely on services of both, microscopic and macroscopic traffic management. A resource

in this context is associated with specific (multi-media) content, which is requested by users. Application Layer Traffic Optimization (ALTO) is also a good example here: this IETF protocol provides guidance to content delivery applications in networks such as P2P or CDN. All the above mentioned categories are associated with mechanisms that may require support from lower layers (below application).

The remaining three building blocks may require only little or no support at all, from the MicTM, MacTM and IRSC. On one hand there is application supported traffic management. There are many applications based on CDN, MSO (Multimedia Streaming Optimization) techniques, and P2P and even P4P (Proactive Network Provider Participation for P2P), which try to optimize performance from end user perspective without getting support from network elements. Another identified building block, called traffic steering usage model, is more relevant from business perspective without bearing many technical aspects. Mainly network operators, but possibly also other stake holders, may influence user behavior by defining certain constraints for usage of networks/services and certain incentives to comply with the usage constraints. Finally, the last identified building block deals with capacity extension in case the available network is regularly in high load conditions. It is a challenge to apply an intelligent planning process for extending the available resources. In contrast to the other building blocks mentioned previously, capacity extension is a process which will become effective in the network after longer time periods, possibly up to several months. In addition to the building blocks there are some common functions like policy control and traffic monitoring.

In the following sections we detail all the derived traffic management building blocks by introducing certain advanced TM solutions as components for integrated traffic management studied inside the scope of MEVICO.

IV. MICROSCOPIC TRAFFIC MANAGEMENT

A. QoS differentiation based on applications and user profiles

The new advanced radio technologies providing real mobile broadband packet data services comparable to the fixed internet and the penetration of smart phones combined together with the flat rate pricing used by the operators have been contributing to the tremendous growth of the mobile data traffic. This makes identification of the type or class of applications essential in traffic management in order to prioritize different application traffic in the network.

There are different techniques for application classification: (1) payload based classification that is based on the inspection of the packet content, and, (2) statistical based classification that consists of analyzing the behavioral and statistical characteristics of the traffic (jitter, session time, inter-arrival time, UL/DL distribution, packet size, etc.). It is a challenging task to classify applications accurately. None of the mentioned methods can provide satisfactory classification of all applications and therefore using together different techniques is typical in modern application classification modules (usually part of DPI systems).

In LTE, policy control is mandatory, meaning that policy enforcement is an essential requirement. This will require DPI functionalities, including application classification. Although, 3GPP standards specified a sophisticated QoS and bearer management model for LTE, it is expected that most Internet traffic will be assigned to the default bearer. In this case, application identification and classification will likely be needed to differentiate and manage internet traffic within the default bearer.

Differentiation of traffic flows for certain applications is increasingly requested and needs to be targeted on a flow or flow class model. This requires the above mentioned classification and detection efforts as well as several means for microscopic traffic management. Commercial and Linux based routers are in general capable of such traffic manipulation, i.e. traffic shaping, dropping, delay management and bit manipulation. In MEVICO it is envisioned to develop a microscopic traffic management framework, which derives the required traffic management actions from application QoS profiles associated with specific application behavior (Skype/YouTube) models. Starting with the application flow detection, it will be possible to lookup the essential QoS parameters thresholds for satisfying QoE levels and to apply the required actions in a distributed fashion.

B. Cross Layer Interference Detection

Interference between adjacent cells is one of the challenging problems in wireless communication. Interference will corrupt packet flows resulting in traffic overhead in the wireless and as well in the wired network [7]. Especially a combination of Automatic Repeat-reQuest (ARQ) based link layer protocols and TCP will suffer from packet losses caused by interference. The link layer tries to hide losses to TCP, not taking into account TCPs retransmission behavior. Every unnecessary TCP retransmission will add unwanted traffic to the network and will reduce application throughput and response times. Similar examples can be found for real time traffic.

Traditional interference situations are detected by mobile end-systems by means of signal strength indicators. End-systems will signal interference situations to the access point the end-system is associated to. The access points can normally not recognize interference, due to the fact that access points will in most cases not interfere with other access points. As commonly known, signal strength indicators depend on the sensitivity of the hardware equipment of the end systems.

In this scenario access points or network devices in the core network, which are located near to the wireless border, will be made capable to identify interference by means of cross layer traffic monitoring. Such devices will stochastically probe specific TCP flows and correlate them by itself and with parameters of lower layer protocols with the aim to identify characteristics of interference. Such methods [8],[9] open the possibility to dynamically reconfigure radio cells to mitigate disturbing interference.

C. Support of multipath flows

A common method to support high bandwidth applications in future mobile architectures is to split a single flow into multiple flows and carry each flow over uncongested regions of the core network. This splitting mechanism can be also used to distribute multiple flows over overlapping radio cells of different radio access networks. This means that the splitting must be done at the end-system. If the flow is carried over a single radio technology, splitting functions can also be placed within the core network. Also a combination of both, end-system and core network splitting support is possible.

Several proposals have been devised aiming to split TCP connections over multiple flows (e.g., [10],[11],[12]), but despite the benefits several issues concerning multipath transport of TCP still remain to be addressed before it can be successfully deployed. MPTCP [13] tries to handle all the open questions: this protocol is considered as the most promising modification of the TCP protocol that supports the simultaneous use of multiple paths between endpoints without any centralized anchor nodes. As a consequence of the multipath the traffic is balanced on the available paths. Fairness is ensured on each path to avoid any starvation on one link. The throughput of the connection is then improved as transmitted data is sent simultaneously on several links. The reliability of the connection is increased as even if one radio link fails, the other links can cope with the data transmission.

But MPTCP still possesses some limitations in the areas of (1) reducing the impact of out-of-order delivery, and (2) relaxing the requirement of support from the end-hosts [14]. In MEVICO we further extend the MPTCP scheme by aiming to address both of the mentioned shortcomings allowing therefore an agnostic TCP over multiple paths solution. We aim to design and implement a transparent proxy solution to increase TCP performance over multiple paths (with different RTTs).

D. Bulk analysis of traffic data

With the introduction of LTE and smart phones, network management for data traffic is becoming a harder problem every day. Data traffic is increasing day by day, it is not easy to keep up with such fast change and the network operator cannot increase the capacity so fast. It is more important than ever before to observe the network and take necessary actions in terms of QoS per applications, hence optimize the network usage for improved customer satisfaction and still remain profitable. Deep packet inspection (DPI) mechanisms are being deployed at the operators, however the amount of investment required inspecting all the traffic in detail is huge. Usually only the traffic which may be important for the operator's business is detected and the rest is not identified.

This shows that some kind of bulk data analysis may prove to be very useful to classify the total data into applications so that the network operator can get to see the big picture. This does not need to be done in real time and not the whole traffic needs to be analyzed, but some time periods can be selected to reflect to the whole week.

One way of doing this is configuring an offline DPI tool and running the bulk samples over this, however this would require very frequent configurations for (1) new sources of existing applications or (2) new application types. Moreover the DPI may not be ready to handle all these changes. Therefore a method is required where traffic is classified into application types (e.g., VoIP, VideoStreaming, P2P, Instant Messaging, Gaming, Web Surfing, etc.) by utilizing traffic characteristics which are common within the classes. In MEVICO the special networking entity called Bulk Analysis Tool (BAT) is proposed to carry this functionality.

V. MACROSCOPIC TRAFFIC MANAGEMENT

A. Core network element selection and reselection

EPS supports resilience (through network element redundancy), optimized routing, balancing of data plane and control plane traffic load in the elements, and sharing of entities among mobile operators. In general the selection process of the core network elements is based on the domain name system (DNS) [15]. The selection entity makes a DNS request to a DNS server to obtain a list of possible network elements. This list is sorted with respect to various criteria (defined in [15], [16]), and then the selection entity chooses the first entry in the sorted list. Besides the initial selection of the core network elements, a reselection might be necessary during operation. Today the main reasons for reselecting network elements are mobility events like tracking area updates and handovers [16]. The optimum selection and reselection of core network elements might be dependent on the currently selected access network. Other reasons for reselection, like load balancing, are not specified in [16] so far, but are subjects of the investigations performed within MEVICO. Also an integrated function which coordinates the selection/reselection procedures for different network elements might improve the overall system performance. To support traffic management also in distributed gateway scenarios it could be beneficial to include additional criteria into the GW selection/reselection procedures like load of the transport and backhaul networks, mobility behavior of users (e.g., low mobile, high mobile), access networks supported by the GWs and the UE, etc. In a future EPS architecture core network element selection and reselection might become more important. This especially holds for distributed architecture realizations where the gateway nodes are located closer to the access network: for highly mobile subscribers the user traffic path via the originally selected gateway entities soon becomes inefficient and a reselection would be favourable.

B. Traffic engineered handovers and network-based IP Flow Mobility (NB-IFOM)

Traffic Engineered Handover (TEHO) techniques focus on decision mechanisms to be involved in RAT changes with a goal not restricted to cope with degradation of signal conditions but also to cover the improvement of traffic conditions in the IP Connectivity Access Network (IP-CAN) together with the improvement and maintenance of the user

QoS/QoE. The two main offloading techniques which support TEHO in reaching the above goals are the IP Flow Mobility (IFOM) [17], [18] and Multi-Access PDN Connectivity (MAPCON) [19]. MAPCON refers to the capability of simultaneously using two or more APNs and enables use cases such as using LTE for QoS demanding applications and WiFi for best effort traffic. IFOM refers to the capability of using the same APN across two wireless access networks (e.g., LTE and WiFi) and enables seamless roaming of applications across different RAT solutions. Currently the key tool to strive IP traffic over a non-3GPP technology is the IEEE 802.21 Media Independent Handover (MIH) standard [20] which provides information and handover assistance services to 3GPP access technologies. Another tool is the Access Network Discovery and Selection Function (ANDSF) specified in [17], [21] for EPS. The ANDSF transfers to the UE the mobile network operator policy rules to connect through non 3GPP access technologies and thus enables a traffic steering that adapts to the QoS and traffic of the controlled LTE network.

The currently standardized IFOM (IP Flow Mobility) solution in 3GPP is strictly UE centric as the operator must firstly deliver the flow routing policies to the UE, and then the UE must provide these policies to the PDN Gateway. Also the ANDSF has no interface to the Policy and Charging Control (PCC) system, therefore it requires other ways to get informed about the updated flow routing policy for a particular UE. In MEVICO we study NB-IFOM (Network-based IP Flow Mobility) solutions in order to eliminate the above limitations and create an operator centric flow management framework. NB-IFOM enables operators to enforce IP flow routing policies without involving the UE first, by letting the PCRF (the central policy control entity) decide on the flow routing policy based on e.g., the available resources in the network, before signaling the policies to the UE. The network-based solution is more efficient than the ones that rely on the UE to perform policy acquisition and enforcement: in the current, UE centric standard it is possible that the network context and resource availability may have changed by the time the UE provides the routing policies to the network; therefore the PCRF will not be able to authorize the new flow policies anymore. Such situations can be avoided if NB-IFOM is applied in the architecture.

C. Multi-Criteria Cell Selection (MCCS)

In next generation networks the architectures are evolving to include cells of different coverage to increase the end user data rate. Mainly, there are two types of cells deployed in hierarchical manner. The first type is a wide area cell (macro cell) that provides moderate date rates for users with above average mobility, and the second type is a local area cell (micro/femto/small cell) that covers a limited area for limited mobility or nomadic users. In case of such deployments end users can access more than one cellular coverage with different load levels, and they have the opportunity to select not only the local cell but also the wide area cells. Previous UE initiated signal-to-noise ratio (SNR) based techniques (e.g., [22], [23]) cannot provide optimal cell selection since those techniques do not consider utilization of the candidate cells. However, this local selection decreases the system capacity since the users only consider the channel quality while selecting their serving cells and ignores the system load information.

Using small cells in the network increases the end-user throughput but it brings extra handoff. Each handoff requires extra signaling and may cause connections failures. Many metrics such as signal strength, distance, SNR, bit error rate (BER), traffic load, quality indicator and some combination of these indicators can be used in order to make handoff decisions in a network-wide and more global manner [24], [25], [26]. Therefore, proper design of cell selection criteria naturally interworking with related 3GPP-specified Self Optimizing Networks (SON) functions such as mobility load balancing (MLB) and mobility robustness optimization (MRO) is a must to achieve efficient load balancing and minimize the number of handoffs in next generation networks.

In MEVICO we investigate various cell selection algorithms based on different criteria for heterogeneous networks and evaluate their suitability for the future mobile communication networks considering the effect on core network.

D. Cell on/off switching, cell site reconfiguration

The increasing amount of traffic is not uniformly distributed in time and spatial dimension [27]. In addition significant amount of power is used for redundant resources. The ratio of this can exceed 20 percent of the original necessary power or can be even higher (according to the given situation) [28]. For energy saving purposes but also for traffic management solutions, the equipment on/off switching meets the requirement of improving efficient usage of network resources. The on/off switching includes not only the switching of the radiated power but it also affects the consumption of other elements of the equipment or in a given segment/area. Current researches on equipment on/off switching apply this power consumption approach and they are rather device oriented [29], [30]. A future objective is to consider, in the decision of cell on/off switching, the impact on the core network, i.e., backhaul utilization, load of distributed S-GWs.

Cell diameter in a given service area is basically designed with fixed parameters assuming a given number of subscribers. However, the increasing number of subscribers, increasing demand on the overall cell capacity and other dynamic effects motivate the application of varying cell ranges, or cell-breathing. The varying cell sizes cause traffic redirections between neighboring cells with effects spreading even towards the S-GW [31]. Despite the fact that the effects of cell breathing on the backhaul and core network segments are also important, research efforts are mainly focused on the radio access network [32], [33]. A future objective is to elaborate RAN TEHO decision strategies which also consider the impact of cell reconfiguration on the core network.

VI. IMPROVED RESOURCE SELECTION AND CACHING

A. Caching improvements and content distribution

A commonly used mechanism to enhance the performance of content delivery networks is caching. Caches have been deployed on the Internet for more than a decade in order to shorten transport paths by making a subset of the most popular web content available near users [34][35][36]. Caches in user equipment can save about 20% of transfer volume [37]. They are most welcome on air interfaces in mobile networks and wherever bandwidth on the last mile is limited and expensive. In addition to shortened round trip time for requested content and load balancing support in the network, the MNO can save interconnect cost due to the reduced amount of data volume received from other network domains. Caching mechanisms can be applied in a way that is transparent or even non-transparent for an application. Also in-line and out-of-band caching can be distinguished: in-line caching means that the entity responsible for caching content is located within the data path, while out-of-band caching implies that a cache is located on a node which is out of the original path.

In addition to "off the shelf" and state of the art caching solutions, it is necessary to analyze optimal deployment strategies for LTE, based on modeling and simulation of network, caching and content popularity parameters. Further optimization of caching can be achieved by considering chunk based storage, content diversity aspects and intelligent cache placement/replacement strategies for e.g., mobility scenarios where the point of convergence between old and new mobility anchor points is further upstream than the cache engine.

Popular content on the Internet is mainly delivered via global CDNs (e.g., Akamai [38], [39]), which shorten the transport paths through distributed server architectures, and via P2P networks. Alternative ways of optimizing traffic paths on CDN and P2P overlays with support from location servers, caches or traffic engineering have been addressed, based on delay measurement. The broadly confirmed relevance of Zipf laws in access patterns is favorable for caching popular content close to users [40]. Avoiding unnecessary traffic load and minimizing delays is a decisive factor for remaining competitive for an upcoming wave of broadband video and IP-TV streaming on the Internet, where hybrid CDN-P2P solutions (like [41]) are the most promising approach for maximizing throughput and exploiting the bandwidth provided in data centers as well as in the broadband access.

B. Resource selection and redirection

Resource selection and redirection is one of the key functional mechanisms to select best suitable resources in P2P and CDN networks [42]. Requested or selected content could be located on/in (1) operator CDN/cache, (2) other localized resource, either end user system or 3rd party provider hosted locally, or (3) external network (content from external CDN, other content provider, end system). Main objectives of resource selection / redirection (i.e., advantages of prioritization between alternative resources and related techniques):

- React dynamically to changed conditions by detecting unfavorable resource usages
- Enable configuration of selection policy
- Re-direction to preferred location
- Constrain load on network resources
- Constrain load on content resources
- Consider impact of events related to user hosted content
- Consider impact of requesting nodes changing point of attachment (access or network)
- Influence selection in external networks

Most re-direction mechanisms used in current CDNs (server-client delivery) are applying DNS and HTTP protocols but there are other schemes like routing, Network Address Translation (NAT), Session Initiation Protocol (SIP), Real Time Streaming Protocol (RTSP), TCP or Application Layer Traffic Optimization (ALTO) based techniques [43][44][45][46].

The envisioned technology in MEVICO aims to facilitate usage of common data sets over different re-direction mechanisms, influence of selection beyond the local MNO domain and detection of unfavorable resource usage.

C. Application Layer Traffic Optimization (ALTO)

The IETF ALTO protocol [46] provides application layer guidance to content delivery applications in networks such as P2P or CDNs, which have to select one or several hosts or endpoints from a set of candidates that are able to provide a desired data resource. This guidance shall be based on parameters that affect performance and efficiency of the data transmission between the hosts, e.g., the topological distance. The ultimate goal is to improve QoS/QoE of the application while reducing resource consumption in the underlying network infrastructure.

While flow movements within the EPS can have an impact on the E2E path and its performance, there is no current way for decision elements within an EPS to anticipate it. Therefore it is necessary to find a way to integrate decision functions in the EPS with knowledge at the E2E scope [47]. To improve its QoE for applications such as video download or streaming, the UE may use the ALTO protocol to jointly optimize the user QoE and the usage of EPS resources by providing the UE with information helping it to choose the best possible location from which to download the whole or piece of content while considering path changes within the EPS.

VII. APPLICATION SUPPORTED TRAFFIC MANAGEMENT

A. P2P optimization techniques: Proactive Network Provider Participation for P2P (P4P)

P4P aims at reducing the load on the network caused by regular P2P traffic. In the regular P2P transmission peers are selected randomly regardless of their location or the link costs. When using P4P, the network provider shares the network topology and corresponding cost map with the P2P application server [48]. With this approach optimal routing (in the view of network provider) and lower end-to-end delay is obtained.

Mobile P4P (mP4P) is the next step in P4P research where the mobile end users share content in a LTE cellular network. LTE mobile environment causes further constraints to P4P such as existence of heterogeneous access networks, frequent joins and leaves of nodes, expectation of efficient signaling and lower complexity algorithms. mP4P will address these issues for optimal routing of content sharing within the LTE/EPC.

Reducing the backbone traffic and lowering the network operation costs are the two main rationales for deploying mobile P4P in LTE/EPC. The P4P iTracker can be easily deployed in the operator's PDN without any hardware modifications in the EPC. The required network map is tracked and stored by the iTracker which shares this information upon the request of the P2P application server.

B. Multimedia streaming optimization (MSO) techniques

Video multimedia has experienced massive growth as a distinct technology from mobile communication, but the globalization and convergence in the mobile communications sector create a merging between mobile communication and video technologies. Therefore an important challenge is the transport of streaming applications in 3GPP mobile networks. In addition to the large amount of traffic generated, streaming applications may show a significantly varying video bitrate over playtime. A significant amount of research has been done in this area (e.g., [49][50]), but they usually lack the evaluation of real-life deployment issues and 3GPP applicability. In MEVCO we propose new elements called MASE (Media Aware Serving Entity) and STME (Steering Traffic Management Entity) to enable the coordination of streaming application requirements and conditions with the bearer resource management in EPS. In addition bottleneck situation in the network can be communicated with the application higher in order to enable adaptation of the video playback to the changed conditions. The introduced components can contribute to a sustained QoE for the user and efficient management of network resources at the same time.

VIII. STEERING USER BEHAVIOR

Functions and techniques related to this traffic management building block deal with business related mechanisms, which can be used by the network operator as a business-driven toolset in order to influence behavior of masses of mobile users. More precisely the traffic usage of users should meet certain pre-defined conditions. On one hand there are conditions for targeted network usage. On the other hand there are incentives in order to influence user behavior to comply with certain rules. The following usage conditions are envisioned:

- (not) to connect to network or specific access points at a certain time
- subscriber stays within a certain traffic volume
- user restricted to certain applications
- user restricts to certain devices
- user restricts to certain usage modes and scenarios

Some of the restrictions are already used today in a rather inflexible way. These conditions may apply in a general way for the user subscription or are bound to a fixed time interval, e.g., on monthly base. This leads to inefficient resource usage. The following incentives could be envisioned:

- reduced charging
- increased traffic priority
- additional services to be used
- different kind of allowances and discounts

A major concern of the used approach is that the notion of 'network neutrality' is violated, which postulates fair treatment of communication services regardless of users, used applications, devices, type of access, etc. A basic challenge for this approach is to make user behavior transparent in order to enable users to react in a proposed way. Usually traffic patterns are influenced by applications, which is non transparent for the user.

IX. DEPLOYMENT OF NEW NETWORKS RESOURCES

Traffic-driven upgrades are a dominant cost factor on fixed and mobile Internet access platforms. As a consequence of traffic growth factors on the wired and wireless broadband Internet, bandwidth provisioning has to be steadily adapted to increasing demands where scalability of technological solutions is desirable to avoid too many shifts to next generation platforms in shortening lifecycle periods. The OPEX and CAPEX expenditures depend on the lifecycle duration of technology generations and on the demand for capacity upgrades, which also refers to implementation expenditures (IMPEX) that are often included in CAPEX. In pure IP networks, link upgrades are usually triggered when a load threshold is exceeded. In order to avoid utilization gaps after upgrades, traffic engineering has to react by redirecting transport paths from links in the surrounding to an upgraded link, such that newly installed bandwidth is instantly exploited to smooth down higher load on other links. Multiprotocol label switching (MPLS) [51] has been developed as a networking sub-layer providing advanced traffic engineering support in meshed IP networks covering a basic set of required functions.

The deployment of new resources (e.g., new or upgraded base stations) can improve coverage up to its capacity limits, while other congested cells in the neighborhood may be able to concentrate on a smaller area to reduce their load. Load balanced paths direct a portion of traffic not on the shortest path and thus may increase the total load when traffic traverses more than the minimum number of links. But the optimization goal of minimizing the maximum load over all links allows only a small amount of deviations to unload congested links and on the other hand allows for a maximum throughput in terms of a linear scaling factor of the traffic matrix.

The optimization tools have to be integrated in a complete traffic engineering cycle for monitoring of the current topology and traffic demand matrix, via re-optimization after relevant shift are observed until reconfiguration of the new adapted path design into the routers [52].

X. Outlook on the Integrated Traffic Management architecture in MEVICO

To achieve resource utilization efficiency for every possible scenario, network operators are on the verge of deploying an integrated traffic management framework aiming to cover all the traffic management building blocks and to organically integrate them into the architecture. In MEVICO the main goal of the traffic management working group is to define the main elements of this framework and to investigate the possible schemes for their efficient interoperation. The analysis of the cooperation of different traffic management solutions and schemes is of particular importance as in some scenarios they might react counteractively. MEVICO's WP4 has already started to investigate these aspects. In the following sections we provide the first insights regarding the potential co-existence of several traffic management techniques.

A. Interactions between MicTM and MacTM

This section provides a first insight about how the traffic management building blocks, MicTM and MacTM, could interact in a layered fashion, as described in Figure 3.

One general service that MicTM mechanisms could offer to MacTM mechanisms is that it passes the traffic measurements, conducted for their own operation. The MacTM mechanisms could aggregate these measurements from many MicTM mechanisms to a coarser resolution and use this as an input parameter. This has the advantage, that fewer measurement functions are needed within the network.

A more specific use case would be, if the MicTM mechanism "Cross Layer Interference Detection" could periodically signal to the MacTM mechanisms "Traffic engineered handovers and network-based IP Flow Mobility" and "Multi-Criteria Cell Selection" the interference situation. These MacTM mechanisms could use this information as an input parameter for their own operation.

B. ALTO and Resource Selection Service

Even though the original purpose of ALTO was to provide relevant information to P2P applications, the framework might be applicable to other contexts as well, such as CDN networks based on a client-server delivery concept. Preference for a specific location and the associated cost can be queried from an ALTO server by an ALTO client. That way the network view can be reflected within the selection process. The resource selection framework followed within the MEVICO project also addresses the problem of un-favorable selection of network resources. Hence the ALTO approach can represent a specific solution but the resource selection framework takes other aspects into consideration as well. Extending the concept of resource query to existing re-direction mechanisms, these have to support an ALTO client implementation. Understanding the impacts of specific extensions for well-known protocols, e.g., ALTO client support integrated into DNS server implementations need further analysis. On the other hand not all re-direction mechanisms follow the query model, which is suggested by ALTO. For instance anycast routers advertise information about preferred routes. Thus ALTO can be considered as a specific solution for the overall problem space of resource selection.

C. Possible conflicts of caching with other traffic management schemes in LTE

Another possible issue is related to the candidate locations of caching servers inside the MNO domain and is strongly connected to the problem space of different MEVICO architecture proposals (i.e., Centralized, Distributed and Flat mobile architectures). The most apparent location of caching nodes is beyond the GTP tunnel endpoint at the SGi interface (e.g., co-located with PDN-GW) or at the S5 interface. The problem here is that placing cache servers there could result in loss of connectivity to the cached material after handovers between 3GPP and non 3GPP accesses. Applying cache nodes at the S1 interface (e.g., co-located with eNodeB) might also be considered, but the benefit of accessing content closer to the users comes along with potential security issues (operators commonly use IPSec) or other limitations (e.g., deployment costs, problems of outdoor deployment). The above motivations make co-location of cache nodes within gateways to be also a promising option.

Besides the possible architectural impacts, the co-location of caching and gateway nodes may also affect gateway re-selection based traffic engineering and/or mobility management mechanisms: if a cache server can be accessed only via a specific gateway node, gateway re-selection and/or mobility management would break the connectivity to the serving cache. Solving this problem would require a complex and presumably costly cache node session transfer protocol. Therefore these mechanisms can co-exist and work simultaneously, if gateway re-selection and mobility management does not force cache server re-selection of a running session.

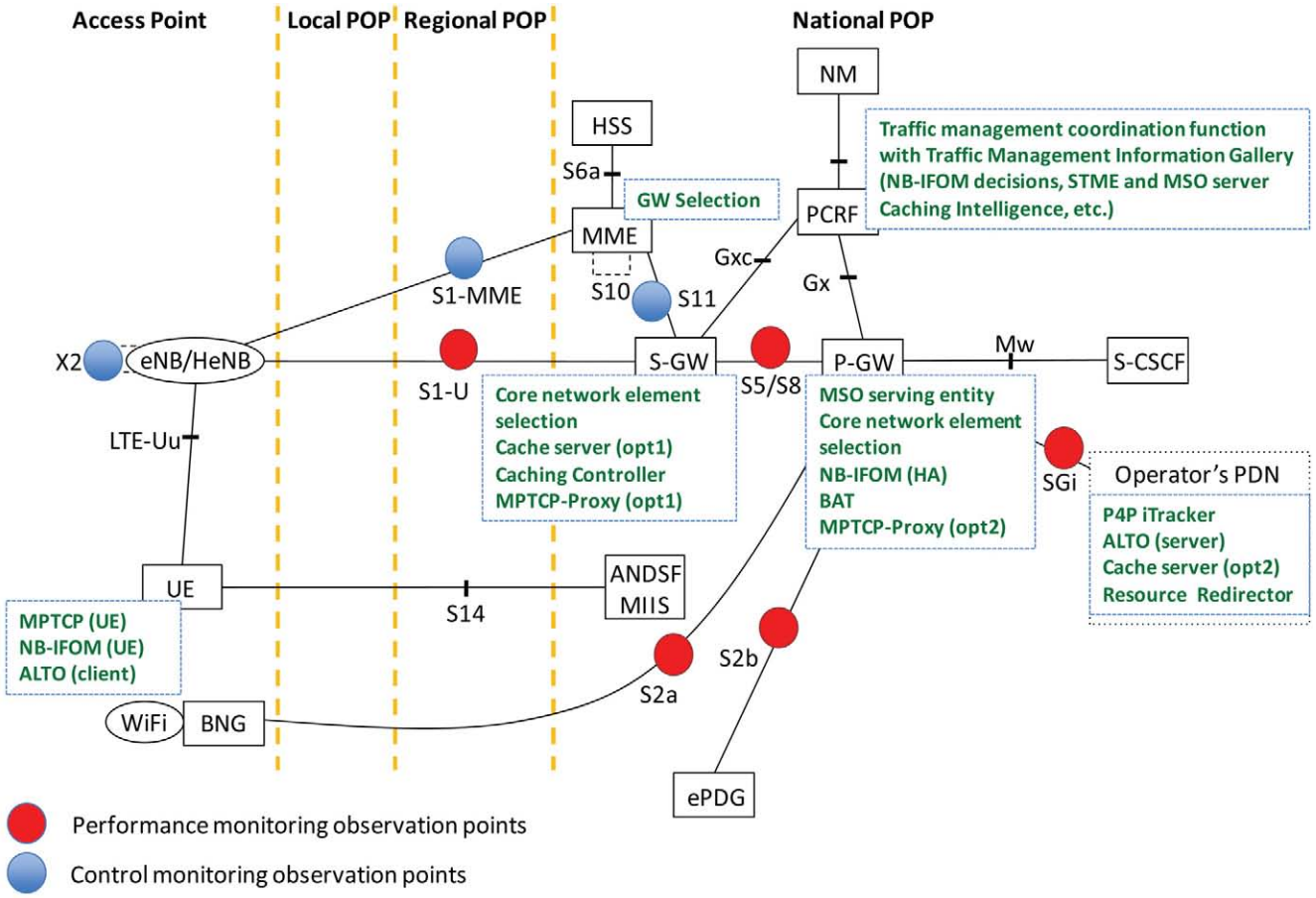


Fig. 4. Outlook on the integrated Traffic Management architecture to be evaluated in MEVICO

Microscopic traffic management schemes and techniques (such as support of multipath communication based on IFOM and/or MPTCP) address operator-centric handling of individual flows. Even though content accessed from a cache node normally doesn't have strict real-time requirements (in terms of latency) there still might be certain quality of experience requirements for the traffic flow associated with the requested cached content. It is therefore a challenge to synchronize the access to the cached content with EPS bearer management and possibly consider additional aspects such as user device characteristics, radio access conditions and other network parameters. Therefore a tighter co-operation might be required between caching and microscopic traffic management solutions at least for some type of cached content.

D. Considerations of a preliminary TM architecture

Traffic management functions tackling the above challenges usually require access to higher layer user plane data, i.e. IP packets, TCP segments and application layer protocols. Placement of such functions at SGi interface or S5 interface are possible options, since GTP tunneling is terminated at these locations. In the following, a brief analysis is done on possible impacts. Positioning of TM functions at S-GW implies that all user plane data can be managed by the considered function unless there is handover between 3GPP and non 3GPP access network. In such case user plane traffic could not be processed or handled by the same node, hosting the TM function. If this can't be avoided, possibly different instances of the TM function have to coordinate in order to ensure continuous TM operation, in case such feature is supported by the TM function in consideration. Positioning the TM function at SGi interface – e.g. co-located with PDN-GW – may cause problems if user data is transferred using different access point names (APN). This usually implies that data paths stretch along different SGi interfaces. It is common practice in currently deployed networks to allocate the same APN to a user for all over-the-top (OTT) services. However managed operator services may use different APNs. As a consequence the same TM function may not be used for connection via different APNs. This situation would increase equipment cost (CAPEX) as well as operational cost (OPEX). As a consequence, the suitable location of TM functions depends on mobility aspects (whether a TM function needs to be supported after 3GPP-non-3GPP handover) or connectivity aspects (whether the same TM function shall be in usage for services using different APN).

XI. CONCLUSION

As mobile and wireless communication architectures evolve toward broadband multiplay and multimedia networks, the demands on the infrastructure increase. Legacy voice, and novel data, video and other applications are to be served on the same network, in the same time. Advanced terminals (i.e., smart phones, tablet PCs and other mobile devices) are spreading and consuming more and more network resources by running their multimedia applications and services. Consequently, the needs for available wireless bandwidth will constantly increase in LTE/LTE-A networks. In such a fast development it is essential that the network must be aware of each application's traffic type and enforce advanced traffic management and control required for ensuring improved Quality of Experience for every user anytime and anywhere. Assuring that mobile and wireless communication systems are application-aware, operators can achieve flexible adaptation to any new application and traffic pattern as soon as they emerge in the future. Mobile operators will be forced by the market to install effective management tools to control every traffic component using enhanced techniques of micro- and macroscopic traffic management, improved resource selection and caching, application supported traffic management, and steering user behavior. Only integrated, advanced traffic management comprising the introduced TM components will ensure that operators can provide cost-effective data transfer with real-time multimedia information over heterogeneous access architectures of future networking schemes.

ACKNOWLEDGMENT

The authors would like to acknowledge the contributions of all of their colleagues in MEVICO, although the views expressed are those of the authors and do not necessarily represent the project. This information reflects the consortium's view, but the consortium is not liable for any use that may be made of any of the information contained therein.

REFERENCES

[1] UMTS Forum, "Magic Mobile Future 2010-2020," UMTS Forum, REPORT NO 37, April 2005.

[2] Cisco VNI, "Global Mobile Data Traffic Forecast Update, 2010-2015," Cisco, Feb. 2011.

[3] Cisco VNI, "Entering the Zettabyte Era," Cisco, June 2011.

[4] M. Dohler, T. Watteyne and J. Alonso-Zárate, "Machine-to-Machine: An Emerging Communication Paradigm," in *GlobeCom'10*, Dec. 2010.

[5] UMTS Forum, "Recognising the Promise of Mobile Broadband," White Paper, June, 2010.

[6] "CELTIC-Plus MEVICO Project (Mobile Networks Evolution for Individual Communications Experience)," [Online]. Available: www.mevico.org. [Accessed 3 January 2012].

[7] M. Fussen, R. Wattenhofer and A. Zollinger, "Interference arises at the receiver," in *Wireless Networks, Communications and Mobile Computing*, 2005.

[8] S. Lohier, Y. Ghamri Doudane and G. Pujolle, "Cross-layer design to improve elastic traffic performance in WLANs," *ACM International Journal of Network Management,* vol. 18, no. 3, July 2008.

[9] S. Shetty, T. Ying and W. Collani, "TCP Venoplus — A cross-layer approach to improve TCP performance in wired-cum-wireless networks using signal strength," in *International Conference of Networking, Sensing and Control (ICNSC)*, 2010.

[10] Y. Lee, I. Park and Y. Choi, "Improving TCP Performance in Multipath Packet Forwarding Networks," *Journal of Communication and Networks (JCN),* vol. 4, no. 2, pp. 148-157, June 2002.

[11] K. Chebrolu, B. Raman and R. R. Rao, "A Network Layer Approach to Enable TCP over Multiple Interfaces," *ACM/Kluwer Journal of Wireless networks (WINET),* vol. 11, no. 5, pp. 637-650, September 2005.

[12] K. Evensen, D. Kaspar, P. Engelstad, A. F. Hansen, C. Griwodz and P. Halvorsen, "A Network-Layer Proxy for Bandwidth Aggregation and Reduction of IP Packet Reordering," in *IEEE 34th Conference on Local Computer Networks (LCN 2009)*, 20-23 October 2009.

[13] A. Ford, C. Raiciu, M. Handley and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses," in *IETF Internet Draft*, draft-ietf-mptcpmultiaddressed-04, July 2011.

[14] A. Kostopoulos, H. Warma, T. Leva, B. Heinrich, A. Ford and L. Eggert, "Towards Multipath TCP Adoption: Challenges and Opportunities," in *6th EURO-NF Conference on Next Generation Internet (NGI)*, Paris, 2-4 June 2010.

[15] 3GPP TS 29.303 V10.2.1, "Domain Name System Procedures, Stage 3, Release 10," 3GPP Technical Specification, July 2011.

[16] 3GPP TS 23.401 V10.4.0, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access, Release 10," 3GPP Technical Specification, June 2011.

[17] 3GPP TS 23.261 V10.1.0, "IP flow mobility and seamless Wireless Local Area Network (WLAN) offload, Stage 2, Release 10," 3GPP Technical Specification, September 2010.

[18] 3GPP TR 23.829 V1.3.0, "Local IP Access and Selected IP Traffic Offload, Release 10," 3GPP Technical Report, Sept. 2010.

[19] 3GPP TR 23.861, "Multi access PDN connectivity and IP flow mobility, Release 9," 3GPP Technical Report, February 2010.

[20] IEEE, "IEEE Standard for Local and metropolitan area networks- Part 21: Media Independent Handover," IEEE Std 802.21-2008, Jan. 2009.

[21] 3GPP TS 23.402 V10.4.0, "Architecture enhancements for non-3GPP accesses, Release 10," 3GPP Technical Specification, June, 2011.

[22] S. V. Hanly, "An algorithm for combined cell-site selection and power control to maximize cellular spread spectrum capacity," *IEEE Journal on Selected Areas in Communications,* vol. 13, no. 7, p. 1332–1340, 1995.

[23] A. Sang, X. Wang, M. Madihian and R. D. Gitlin, "A Load-aware handoff and cell-site selection scheme in multi-cell packet data systems," in *IEEE 47th Global Telecommunications Conference (GLOBECOM)*, 2004.

[24] D. Amzallag and et al., "Cell selection in 4G cellular networks," in *IEEE Conference on Computer Communications*, 2008.

[25] J.-M. Moon and D.-H. Cho, "Efficient Cell Selection Algorithm in Hierarchical Cellular Networks: Multi-User Coordination," *IEEE Communication Letters,* vol. 14, no. 2, February 2010.

[26] C.-J. Chang, C.-Y. Hsieh and Y.-H. Chen, "A Preference Value-Based Cell Selection Scheme in Heterogeneous Wireless Networks," in *IEEE WCNC*, 2010.

[27] S. Almeida, J. Queijo and L. Correia, "Spatial and temporal traffic distribution models for GSM," Vehicular Technology Conference, VTC 1999 - Fall, 1999.

[28] E. Oh and et al., "Toward Dynamic Energy-Efficient Operation of Cellular Network Infrastructure," *IEEE Communications Magazine,* pp. 56-61, June 2011.

[29] A. Tuffery and et al., "A 27.5-dBm linear reconfigurable CMOS power amplifier for 3GPP LTE applications," in *IEEE New Circuits and Systems Conference (NEWCAS)*, Bordeaux, France, 26-29 June 2011.

[30] D. Y. Cl., "RF IC design of highly-efficient broadband polar transmitters for WiMAX and 3GPP LTE applications," in *IEEE Solid-State and Integrated Circuit Technology (ICSICT)*, Shanghai, China, 1-4 November 2010.

[31] R. Kwan, R. Arnott and et al., "On Mobility Load Balancing for LTE Systems," in *Vehicular Technology Conference Fall (VTC 2010-Fall)*, 2010.

[32] J. Pérez-Romero and et al., "Network-Controlled Cell-Breathing for Capacity Improvement in Heterogeneous CDMA/TDMA Scenarios," in *WCNC*, Las Vegas, 3-6 April 2006.

[33] S. Bhaumik, G. Narlikar, S. Chattopadhyay and S. Kanugovi, "Breathe to Stay Cool: Adjusting Cell Sizes to Reduce Energy Consumption," in *ACM SIGCOMM Green Networking*, New Delhi, India, 30 August - 3 September, 2010.

[34] G. Barish and K. Obrazcka, "World wide web caching: Trends and techniques," *IEEE Communications Magazine,* pp. 178-185, May 2000.

[35] R. Fielding and et al., "HTTP/1.1, part 6: Caching," IETF Internet-Draft, draft-ietf-httpbis-p6-cache-18, January 4, 2012.

[36] G. Haßlinger and O. Hohlfeld, "Efficiency of caches for content distribution on the Internet," in *22. Internat. Teletraffic Congress*, Amsterdam, The Netherlands, 2010.

[37] J. Charzinski, "Traffic properties, client side cachability and CDN usage of popular web sites," in *15th MMB conference*, Essen, Germany, 2010.

[38] Akamai, "State of the Internet, Quarterly Report Series (2011)," 2011. [Online]. Available: www.akamai.com. [Accessed 3 January 2012].

[39] A.-J. Su, D. Choffnes, A. Kuzmanovic and F. Bustamante, "Drafting behind Akamai," *IEEE/ACM Trans. on Networking,* vol. 17, p. 1752–1765, 2009.

[40] L. Breslau and et al., "Web caching and Zipf-like distributions: Evidence and implications," in *IEEE Infocom*, 1999.

[41] C. Huang, A. Wang, J. Li and K. Ross, "Understanding hybrid CDN-P2P," in *NOSSDAV Conf*, Braunschweig, Germany, 2008.

[42] R. Torres, A. Finamore, K. Jin Ryong, M. Mellia, M. M. Munafo and S. Rao, "Dissecting Video Server Selection Strategies in the YouTube CDN," June 2011.

[43] H. A. Alzoubi, S. Lee, M. Rabinovich, O. Spatscheck and J. E. van der Merwe, "Anycast CDNS revisited," in *WWW 2008 / Refereed Track: Performance and Scalability*, Beijing, China, April 21-25, 2008.

[44] Apache web server, "Apache web server module “mod_rewrite”," [Online]. Available: http://httpd.apache.org/docs/2.2/mod/mod_rewrite.html. [Accessed 3 January 2012].

[45] DynDNS, "Dynamic DNS," [Online]. Available: http://www.webopedia.com/TERM/D/dynamic_DNS.html. [Accessed 3 January 2012].

[46] R. Alimi and et al., "ALTO Protocol," IETF Internet Draft, draft-ietf-alto-protocol-10.txt, October 31, 2011.

[47] Y. El Mghazli, S. Randriamasy and F. Taburet, "ALTO in Mobile Core," IETF Internet Draft, draft-randriamasy-alto-mobile-core-01, October 23, 2010.

[48] H. Xie, Y. Yang, A. Krishnamurthy, Y. Liu and A. Silberschatz, "P4P:Provider portal for P2P applications," in *ACM SIGCOMM*, 2008.

[49] R. Fracchia and et al., "System architecture for multimedia streaming optimisation," in *Future Network and Mobile Summit*, Firenze, Italy, 16-18 June 2010.

[50] C. Lamy-Bergot, G. Panza, A. Rotondi and L. Fratta, "Analysis and Optimization of a JSCC/D System on 4G Networks," in *IEEE International Symposium on Spread Spectrum Techniques and Applications*, Bologna, Italy, August 2008.

[51] E. Rosen, A. Viswanathan and R. Callon, "Multiprotocol Label Switching Architecture," IETF RFC 3031, January 2001.

[52] G. Haßlinger, S. Schnitter and M. Franzke, "The Efficiency of Traffic Engineering with Regard to Failure Resilience," *Telecommunication Systems,* vol. 29, no. 2, pp. 109-130, 2005.

László Bokor graduated in 2004 with M.Sc. degree in computer engineering from the Budapest University of Technology and Economics (BME) at the Department of Telecommunications. In 2006 he got an M.Sc.+ degree in bank informatics from the same university’s Faculty of Economic and Social Sciences. He is a Ph.D. candidate at BME, member of the IEEE, member of Multimedia Networks Laboratory and Mobile Innovation Centre of BME where he participates in researches of wireless protocols and works on advanced mobility management related projects (as FP6-IST PHOENIX and ANEMONE, EUREKA-Celtic BOSS, FP7-ICT OPTIMIX, EURESCOM P1857, EUREKA-Celtic MEVICO, FP7-ICT CONCERTO). His research interests include IPv6 mobility, next generation networks, mobile broadband networking architectures, network performance analyzing, and heterogeneous networks.

Zoltán Faigl received his MSc degree in Telecommunications from Budapest University of Technology and Economics (BME), Hungary in 2003. Currently he works on his PhD at the Mobile Innovation Centre at BME. His fields of interests are communication protocols, network architectures, information security, mobile and wireless networks, network dimensioning. He participates in researches of wireless protocols and works on advanced mobility management related projects (as FP5-IST NEWCOM, FP6-IST PHOENIX and ANEMONE, EURESCOM P1857, EUREKA-Celtic MEVICO).

Jochen Eisl received his MSc degree in Information and Communication Technology from Technical University of Munich, Germany in 1992. He started his career at Siemens Telecommunication Group with system engineering and software development for telecom management systems. Since 1997 he plays a very active role in various European (FP4, FP5, FP7), national (BMBF) and company internal research projects. In 2000 his focus shifted towards public mobile networks, with a special expertise on packet core. His duties are project coordination with internal and external partners, technical and strategy analysis, consulting and managing research liaisons. His special interest since 2009 is on optimization on content delivery and streaming support in LTE networks. So far he is an author of 36 publications and 23 patent filings.

Gerd Windisch received his "Diplom-Ingenieur"-Degree in Information and Communication Technology from Chemnitz University of Technology (CUT) in 2008. He is currently a research assistant at the Chair for Communication Networks at CUT and is working on his Ph.D. in Information and Communication Technology. His main research interests are macroscopic traffic management mechanisms in mobile core networks. He focuses on optimized gateway selection, novel mechanisms for gateway reselection and core network offloading mechanisms. Currently, he is participating in the EUREKA-Celtic project MEVICO.

Guidelines for our Authors

Format of the manuscripts

Original manuscripts and final versions of papers should be submitted in IEEE format according to the formatting instructions available on
http://www.ieee.org/publications_standards/publications/authors/authors_journals.html#sect2,
"Template and Instructions on How to Create Your Paper".

Length of the manuscripts

The length of papers in the aforementioned format should be 6-8 journal pages.
Wherever appropriate, include 1-2 figures or tables per journal page.

Paper structure

Papers should follow the standard structure, consisting of *Introduction* (the part of paper numbered by "1"), and *Conclusion* (the last numbered part) and several *Sections* in between.
The Introduction should introduce the topic, tell why the subject of the paper is important, summarize the state of the art with references to existing works and underline the main innovative results of the paper. The Introduction should conclude with outlining the structure of the paper.

Accompanying parts

Papers should be accompanied by an *Abstract* and a few *index terms (Keywords)*. For the final version of accepted papers, please send the *short cvs* and *photos* of the authors as well.

Authors

In the title of the paper, authors are listed in the order given in the submitted manuscript. Their full affiliations and e-mail addresses will be given in a footnote on the first page as shown in the template. No degrees or other titles of the authors are given. Memberships of IEEE, HTE and other professional societies will be indicated so please supply this information.
When submitting the manuscript, one of the authors should be indicated as corresponding author providing his/her postal address, fax number and telephone number for eventual correspondence and communication with the Editorial Board.

References

References should be listed at the end of the paper in the IEEE format, see below:

a) Last name of author or authors and first name or initials, or name of organization
b) Title of article in quotation marks
c) Title of periodical in full and set in italics
d) Volume, number, and, if available, part
e) First and last pages of article
f) Date of issue

[11] Boggs, S.A. and Fujimoto, N., "Techniques and instrumentation for measurement of transients in gas-insulated switchgear," IEEE Transactions on Electrical Installation, vol. ET-19, no. 2, pp.87–92, April 1984.

Format of a book reference:

[26] Peck, R.B., Hanson, W.E., and Thornburn, T.H., Foundation Engineering, 2nd ed. New York: McGraw-Hill, 1972, pp.230–292.

All references should be referred by the corresponding numbers in the text.

Figures

Figures should be black-and-white, clear, and drawn by the authors. Do not use figures or pictures downloaded from the Internet. Figures and pictures should be submitted also as separate files. Captions are obligatory. Within the text, references should be made by figure numbers, e.g. "see Fig. 2."
When using figures from other printed materials, exact references and note on copyright should be included. Obtaining the copyright is the responsibility of authors.

Contact address

Authors are requested to send their manuscripts via electronic mail or on an electronic medium such as a CD by mail to the Editor-in-Chief:

Csaba A. Szabo
Dept. of Telecommunications
Budapest University of Technology and Economics
2 Magyar Tudosok krt.
Budapest 1117 Hungary
szabo@hit.bme.hu

Our reviewers in 2011

The quality of a research journal depends largely on its reviewing process and, first of all, on the professional service of its reviewers. It is my pleasure to publish the list of our reviewers in 2010 and would like to express my gratitude to them for their devoted work.

Your Editor-in-Chief

Luigi Atzori,
University of Cagliari, Italy

László Bokor,
BME, Hungary

Levente Buttyán,
BME, Hungary

Iacopo Carreras,
CREATE-NET, Italy

Tibor Cinkler,
BME, Hungary

George Dan,
Royal Technical University, Stockholm, Sweden

Franco Davoli,
University of Genova, Italy

Virgil Dobrota,
Technical University Cluj, Romania

Károly Farkas,
BME, Hungary

Kálmán Fazekas,
BME, Hungary

Péter Fazekas,
BME, Hungary

Zsolt Félegyházi,
BME, Hungary

Enrico Gregori,
CNR IIT, Pisa, Italy

Antonio Grilo,
INOV, Lisbon, Portugal

Christian Guetl,
University of Graz, Austria

Lajos Hanzo,
University of Southampton, UK

Gábor Horváth,
BME-HIT, Hungary

Gábor Horváth,
BME-MIT, Hungary

Sándor Imre,
BME, Hungary

Thomas Heistracher,
Salzburg University of Applied Sciences, Austria

László T. Kóczy,
Széchenyi University of Győr, Hungary

János Levendovszky,
BME, Hungary

László Lois,
BME, Hungary

Oscar Mayora,
CREATE-NET, Italy

Szilvia Nagy,
Széchenyi University of Győr, Hungary

László Osváth,
BME, Hungary

Gábor Tamás Orosz,
BME, Hungary

László Pap,
BME, Hungary

Tatiana Polischuk,
HIIT, Finland

Csaba A. Szabó,
BME, Hungary

Tibor Szkaliczki,
SZTAKI, Hungary

János Sztrik,
University of Debrecen, Hungary

Jan Turan,
Technical University of Kosice, Slovakia

Gergely Zaruba,
University of Texas as Arlington, USA

Honggang Zhang,
Zheijang University, China

Adam Wolisz,
Technical University of Berlin, Germany

(* BME – Budapest University of Technology and Economics)

Contents of the Infocommunications Journal 2011 (Volume III)

2011/1 *Infocommunications Journal*

2011/2 *Infocommunications Journal*

2011/3 *Infocommunications Journal*

2011/4 *Infocommunications Journal*

IEEE INTERNATIONAL CONFERENCE ON COMMUNICATIONS

ICC 2013

Bridging the Broadband Divide
9-13 June • Budapest, Hungary

IEEE | IEEE COMMUNICATIONS SOCIETY

WWW.IEEE-ICC.ORG/2013

CALL FOR PAPERS

The 2013 IEEE International Conference on Communications (ICC) will be held in the vibrant city of Budapest, Hungary from 9 – 13 June 2013. This flagship conference of IEEE Communications Society aims at addressing an essential theme on "Bridging the Broadband Divide." The conference will feature a comprehensive technical program including several Symposia and a number of Tutorials and Workshops. IEEE ICC 2013 will also include an attractive expo program including keynote speakers, various Business, Technology and Industry fora, and vendor exhibits. We invite you to submit your original technical papers, industry forum, workshop, and tutorial proposals to this event. Accepted and presented papers will be published in the IEEE ICC 2013 Conference Proceedings and in IEEE Xplore®. Full details of submission procedures are available at http://www.ieee-icc.org/2013.

To be published in the IEEE ICC 2013 Conference Proceedings and IEEE Xplore®, an author of an accepted paper is required to register for the conference at the full member or non-member rate and the paper must be presented at the conference. Non-refundable registration fees must be paid prior to uploading the final IEEE formatted, publication-ready version of the paper. For authors with multiple accepted papers, one full registration is valid for up to 3 papers. Accepted and presented papers will be published in the IEEE ICC 2013 Conference Proceedings and in IEEE Xplore®.

PLANNED TECHNICAL SYMPOSIA

Selected Areas in Communications Symposium

E-Health Area
Pradeep Ray, University of New South Wales, Australia

Power Line Communications Area
Andrea Tonello, University of Udine, Italy
Stephan Weiss, University of Strathclyde, UK

Smart Grids Area
Bahram Honary, Lancaster University, UK

Tactical Communications & Operations Area
Gabe Jakobson, Altusys, USA

Satellite & Space Communication Area
Hiromitsu Wakana, NICT, Japan

Data Storage Area
Tiffany Jing Li, Lehigh University, USA

Access Systems and Networks Area
Michael Peeters, Alcatel-Lucent, Belgium

Green Communication Systems and Networks
Athanassios Manikas, Imperial College London, UK

Wireless Communications Symposium

Zhaocheng Wang, Tsinghua University, China
Metha B. Neelesh, Indian Institute of Science, India
Hanna Bogucka, Poznan University of Technology, Poland
Fredrik Tufvesson, Lund University, Sweden

Wireless Networking Symposium

Azzedine Boukerche, University of Ottawa, Canada
Pan Li, Mississippi State University, USA
Min Chen, Seoul National Unversity, Korea

Communication Theory Symposium

David Gesbert, EURECOM, France
Angel Lozano, Universitat Pompeu Fabra, Spain
Velio Tralli, University of Ferrara, Italy
Sennur Ulukus, University of Maryland, USA

Signal Processing for Communications Symposium

Hai Lin, Osaka Prefecture University, Japan
Octavia Dobre, Memorial University, Canada
Saiid Boussakta, Newcastle University, UK
Hongyang Chen, Fujitsu Laboratories, Japan

Optical Networks and Systems Symposium

Xavier Masip-Bruin, Technical University of Catalonia, Spain
Franco Callegati, University of Bologna, Italy
Tibor Cinkler, Budapest University of Technology and Economics, Hungary

Next-Generation Networking Symposium

Malathi "MV" Veeraraghavan, University of Virginia, USA
Joel Rodrigues, University of Beira Interior, Portugal
Wojciech Kabacinski, Poznan University of Technology, Poland

Communication QoS, Reliability & Modeling Symposium

Tetsuya Yokotani, Mitsubishi Electric Corporation, Japan
Harry Skianis, University of the Aegean, Greece
Janos Tapolcai, Budapest University of Technology and Economics, Hungary

Ad-hoc and Sensor Networking Symposium

Guoliang Xue, Arizona State University, USA
Abdallah Shami, University of Western Ontario, Canada
Xinbing Wang, Shanghai Jiaotong University, China

Communication Software and Services Symposium

Jiangtao (Gene) Wen, Tsinghua University, China
Lynda Mokdad, University Paris-Est, France

Communication and Information Systems Security Symposium

Tansu Alpcan, TU Berlin, Germany
Mark Felegyhazi, Budapest University of Technology and Economics, Hungary
Kejie Lu, University of Puerto Rico at Mayagüez, PR

Cognitive Radio and Networks Symposium

Honggang Zhang, Zhejiang University, China
David Grace, University of York, UK
Andrea Giorgetti, University of Bologna, Italy

COMMITTEE

General Chair:
Christopher Mattheisen
Magyar Telekom, Hungary

Executive Chair:
Lajos Hanzo
University of Southampton, UK

Technical Program Chair:
Andreas Molisch
University of Southern California, USA

Technical Program Vice-Chairs:
Andrea Conti
University of Ferrara, Italy

Iain Collings
CSIRO ICT Centre, Australia

Workshops Co-Chairs:
Thomas Michael Bohnert
Zurich University of Applied Sciences, Switzerland

Christoph Mecklenbrauker
Vienna University of Technology, Austria

Christina Fragouli
EPFL, Switzerland

Tutorials Co-Chairs:
Marco Chiani
University of Bologna, Italy

Wei Chen
Tsinghua University, China

Panel Session Co-Chairs:
David Soldani
Huawei, Germany

Peter Rost
NEC Labs Europe, Germany

Publications Co-Chairs:
Dong In Kim
Sungkyunkwan University, Korea

Peter Mueller
IBM Zurich Research Laboratory, Switzerland

Conference Operations Chair:
Rolland Vida
Budapest University of Technology and Economics, Hungary

Patronage Chair:
Roland Jakab
Ericsson, Hungary

Keynotes Co-Chairs:
Doug Zuckerman
Telcordia, USA

Gerhard Bauch
Universität der Bundeswehr München, Germany

Finance Chair:
Peter Nagy
HTE, Hungary

Publicity Chair:
John Vig
IEEE, USA

Local Arrangements Chair:
Nandor Matrai
Asszisztencia, Hungary

IMPORTANT DATES

Paper Submission	Acceptance Notification	Camera-Ready	Tutorial Proposal	Workshop Proposal:	Business Forum Proposal
16 September 2012	27 January 2013	24 February 2013	7 October 2012	18 March 2012	8 April 2012

SCIENTIFIC ASSOCIATION FOR INFOCOMMUNICATIONS

Who we are

Founded in 1949, the Scientific Association for Infocommunications (formerly known as Scientific Society for Telecommunications) is a voluntary and autonomous professional society of engineers and economists, researchers and businessmen, managers and educational, regulatory and other professionals working in the fields of telecommunications, broadcasting, electronics, information and media technologies in Hungary.

Besides its more than 1300 individual members, the Scientific Association for Infocommunications (in Hungarian: HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET, HTE) has more than 60 corporate members as well. Among them there are large companies and small-and-medium enterprises with industrial, trade, service-providing, research and development activities, as well as educational institutions and research centers.

HTE is a Sister Society of the Institute of Electrical and Electronics Engineers, Inc. (IEEE) and the IEEE Communications Society. HTE is corporate member of International Telecommunications Society (ITS).

What we do

HTE has a broad range of activities that aim to promote the convergence of information and communication technologies and the deployment of synergic applications and services, to broaden the knowledge and skills of our members, to facilitate the exchange of ideas and experiences, as well as to integrate and harmonize the professional opinions and standpoints derived from various group interests and market dynamics.

To achieve these goals, we…

- contribute to the analysis of technical, economic, and social questions related to our field of competence, and forward the synthesized opinion of our experts to scientific, legislative, industrial and educational organizations and institutions;
- follow the national and international trends and results related to our field of competence, foster the professional and business relations between foreign and Hungarian companies and institutes;
- organize an extensive range of lectures, seminars, debates, conferences, exhibitions, company presentations, and club events in order to transfer and deploy scientific, technical and economic knowledge and skills;
- promote professional secondary and higher education and take active part in the development of professional education, teaching and training;
- establish and maintain relations with other domestic and foreign fellow associations, IEEE sister societies;
- award prizes for outstanding scientific, educational, managerial, commercial and/or societal activities and achievements in the fields of infocommunication.

Contact information

President: **DR. GÁBOR HUSZTY** • *ghuszty@entel.hu*

Secretary-General: **DR. ISTVÁN BARTOLITS** • *bartolits@nmhh.hu*

Managing Director, Deputy Secretary-General: **PÉTER NAGY** • *nagy.peter@hte.hu*

International Affairs: **ROLLAND VIDA, PhD** • *vida@tmit.bme.hu*

Addresses

Office: H-1055 Budapest, V. Kossuth Lajos square 6-8, Room: 422.

Mail Address: 1372 Budapest, Pf. 451., Hungary

Phone: +36 1 353 1027, Fax: +36 1 353 0451

E-mail: *info@hte.hu*, Web: *www.hte.hu*