MŰEGYETEM 1782

Some problems and its solutions of networked communication and interworking

Tentative preliminary title

Summary of the new results of the Ph.D. thesis

Gábor Ziegler

High Speed Networks Laboratory
Department of Telecommunication and Telematics
Budapest University of Technology and Telematics

19th November 2004

Supervisors

Dr. András Lőrincz
Department of Information Systems
Eötvös Loránd University of Sciense s

Dr. Csilla Farkas
Department of Computer Science and Engineering
University of South Carolina

Dr. János Miskolczi
now with Ericsson Hungary Ltd, formerly at
Research Institute for Measurement and Computing Techniques within the
Central Research Inistitute for Physics of the Hungarian Academy of Scienses

Budapest, Hungary
2004

File `Id: titlepage.tex,v 1.7 2004/11/13 08:47:57 ziegler Exp`

Contents

1 Introduction

Traditionally there were many different purpose communication networks using many different, dedicated technologies. The current trend in telecommunication is "convergence", which almost became an over-used stereotype.

This process began first in the "telecom-world", that is, the classical, circuit-switched telephone network, which was originally speech oriented. This continued by embracing non-speech communication, such as circuit-switched data communication (e.g., telex, then facsimile services). Later packet-switching started to spread (e.g. X.25 networks) and this convergence culminated in the concept of Integrated Services Digital Networks[1, 2, 3]. The next logical step was the introduction of Mobile Networks, such as GSM [4].

Meanwhile, "datacom networks" (that is, packet-switched data-communication networks) gained momentum from the advent of computers: the need has arisen for machine-to-machine communication without human intervention, such as Unix-to-Unix-Copy (UUCP) [5]. This has eventually evolved into the web of data-communications network that we commonly refer to as the Internet [6].

As the packet-switched technology matured it is becoming more and more viable to converge these different technologies, resulting in such new solutions that Voice-over-IP (VoIP) [7].

The future of the communication networks doubtlessly lies within full convergence, such the IMT-2000[8] initiative of the ITU-T [9], or its European version, the Universal Mobile Telecommunication System (UMTS) [10] developed by 3GPP[11] and ETSI [12].

This convergence undoubtedly results in a complex and heterogeneous network environment and poses many challenging technical problems to solve. In my dissertation I deal with certain problems of the above mentioned technologies, which are loosely coupled to each other.

In the rest of this Introduction I overview my research objectives and methodology in Sections 1.1 and 1.2, then I depict the structure, or "glue" of my thesis in Section 2 that interconnects the individual thesis-claim groups. In Section 3 I describe my new scientific results. These are organized into three main thesis-claim groups, corresponding to their introductory discussions in Section 2.

1.1 Research objectives

In my research I was always interested in the problems of communication systems. The Internet is more and more involved in our everyday life and seems to merge with other communication systems to form a joint communication-infosphere around us. This huge and fast evolution poses challenging questions in different fields. In my view, these different facets can not be considered separately: a common view seems necessary to unite the different and sometimes contradictory facets of this evolution. Several key problems could be addressed, the three key points I consider most important are the followings:

- Internet has become almost the primary source of information, which improved the importance of several:
  - intelligent, human and robotic community based data mining techniques are of high importance
  - privacy and personal rights have to be protected, since these are more vulnerable in on-line environments, contrary to the widespread belief of the "anonymity" of the Internet,
  - the current widespread use of false and malicious information distribution (e.g., spam, phising, stb.) calls for certain degree of enforceable accountability
- All of the algorithms and their host hardware (at least in theory) should be error free:
  - testing and optimization are necessary throughout the entire life-cycle of the products (either hardware, or software), including the design phase before the actual manufacturing or development.

  - testing in simulated working conditions is often useful and necessary at the same time

- The exponential growth of the testing steps with the number of units requires novel state-of-the-art methods.

My three main thesis-claims of my dissertation try to cover these three fields, respectively. My research has been conducted on these fields while I was also engaged in practical engineering works. During these years some of my claims presented/repeated in this dissertation might have been improved by other researchers, however, at the time of their first publication they were new.

The understanding I gained during my research work, which allowed me to formulate the central problems in a top-down manner also allowed me to keep track the recent development on these particular and still most important points. To each claims, I will add a short description, or at least some references about the state-of-the-art today.

I first discuss the dual problem of anonymity and accountability over the Internet in thesis claim-group 1. It is discussed in Section 2.1 and detailed in Section 3.1, see also [J1, C3].

The above proposed solution has a distributed nature. I was always fascinated by the possibilities and inherent testability problems of the layered Open Systems Interconnection [13] model, which provided the first viable and implementable model of distributed systems having heterogeneous components. This will guide me toward the thesis claim-group 2, which is related to protocol testing practices using trace analysis. It is discussed in 2.2 and detailed in 3.4, see also [D1, J4, J5, C4, C6].

Communications protocol testing, especially computer aided test generation (CATG) [C4] often suffers from exponential growth of the generated test sequences. This problem can be tackled, for example, by optimization techniques, see, e.g., [14].

The last part of my thesis therefore discusses the possibilities of combining two optimization algorithms: Stage [15] and the Genetic Algorithm with Local Search [16]. This has resulted in the thesis claim-group 3, which is discussed in 2.3 and detailed in Section 3.5, see also [J6, J2, C7]. The aim of the combination of these two algorithms was to mix the "robustness" of the Genetic Algorithms and the "intuitiveness" of Stage.

1.2 Research methods

Any credible research should start with an overview of the scientific state-of-the-art by appropriate literature search. This has been conducted for each three fields of my research, as documented in [C3], [D1] and [J6].

Theoretical analysis of the layered architecture was performed for the claim-groups 1 and 2. The former claim-group has underwent the trial of actual implementation effort [17], while the latter has underwent the scrutiny of a public-defense process [D1].

The claim-group 3 was exposed to another traditional research method: controlled simulations have been performed to evaluate of the effectiveness of the proposed algorithm [J6].

2 Challanges in modern telecommuncations

2.1 Challanges of the accountable cooperation with anonymity

One of the most fascinating possibilities of the World Wide Web and its underlying communication infrastructure, the Internet, is their support of (electronic) collaboration beyond the traditional geographical limits. A key factor of these collaborations is their "virtuality", that is, instead of real users their *virtual identities* are observable. The need to provide privacy in this virtual world led to the development of several theoretical research as well prototype implementations. These technologies provide data or communications anonymity or personalization

For example, Onion Routing [18], Crowds [19], and Hordes [20] provide connection anonymity. Systems GNUnet [21], FreeNet [22], and Napster [23] facilitate file-sharing services and guarantee different levels of anonymity. Models, like anonymous e-mail [24, 25] or electronic commerce [26, 27, 28], have been developed to support specific applications. My claim is that full anonymity poses a serious security problem, allowing malicious users to avoid accountability for their actions.

I proposed [J1, C3] a multi-layered framework that supports anonymous collaborations of virtual users while providing means to hold them responsible for their activities. I use the term *accountability* for this latter requirement throughout this booklet. I use *pseudonymity* to hide the identity of a user but allow to reveal this identity under specific circumstances. The main focus of my work is to develop methods that guarantee that the mapping between a user's identity and the corresponding pseudonym cannot be disclosed, unless this disclosure is justified. This *justification* may be given by the virtual community (e.g., to enforce internal requirements) or by the external *society* of the community (e.g., to enforce legal restrictions).

Most of the existing works require a trusted authority or authorities to safeguard these mappings. A limitation of these approaches is that it is not always possible to find such entities. I proposed a new method that distributes trust among the members of the community rather than requiring the existence of a single trusted entity. The disclosure of a user's identity requires the collaboration of a quorum of users. My techniques guarantee accountability and high-assurance anonymity.

2.1.1 Differentiating between internal and external accountability

I proposed a two-layered anonymity model. The first layer provides mapping among the different virtual identities of the same real user, without revealing the identity of the real user. The second layer provides mapping between a real user and the user's base virtual identity. To reveal the mapping at each layer, the support of the community is required. Disclosure of the mapping between a real user and the corresponding base identity also requires external justification, like court order. Therefore, I have developed the concepts of *internal* and *external* accountability.

1. *Internal accountability* is when the virtual (pseudonym) member of a group is identifiable within the group and can be held responsible for his/her actions according to the "ethic", or policy of the group.

2. *External accountability* when the real entity behind the pseudonym member of a group is identifiable and can be held responsible for his/her actions according to

the “ethic”, or the law of the external environment hosting the group.

The problem of deciding who is allowed to issue a justification to reveal the above mappings is outside of the scope of this thesis.

2.1.2 A solution with threshold cryptography

I am concerned with the technology, which (i) is capable of handling requests from the external world, (ii) offers the tools for investigating inconsistencies of the internal decision making, (iii) can keep the anonymity of the investigators and, (iv) which, under certain conditions, can implement new rules that modify decision making. The computational challenge is how to define such communities and how to safeguard the operations. This is currently (in 2004) an ongoing research topic among three universities (BME and ELTE from Hungary and USC from USA). Our initial results were presented in [C3]. We also provided means to the users to look at the data stored about them. Behind issues of accountability and anonymity the system is capable to realize a democratic, self-organizing community where the rights (e.g., access control) can be issued and distributed automatically based on the “merits” of the members.

2.1.3 The prototype project: SyllabNet

I also present my experimental implementation, a “practical choice” of these concepts for a real world application [17]. In my example, students can evaluate course materials, can design their own course maps using a graphical map editor, have a map publishing web application, and can keep their anonymity under A2SOC principles. Internal accountability means that individual maps, their annotations, forum entries, etc. can be evaluated by the community and the *value* can be associated or mapped to virtual user identities in a non-ambiguous fashion. External accountability concerns those participants of the community, whose role need to be changed. One example is that the activity of a virtual user is not allowed by the rules of the community and this person should be excluded from publishing. Another – not yet implemented – option is that a Board makes decisions if maps meet certain criteria and can be published or not.

Such refereeing constrains anonymity: the author and the referee should be different real persons.

Novel aspects of my work include

- the formalization of A2SOC systems,
- the improvement of the original cryptographic protocol from using one central trusted entity to two semi-trusted entities.

These are published in [J1] and detailed in Section 3.1.

2.2 Trace analysis in conformance testing of telecommunication protocols

Modern Internet based systems often have distributed architecture, which means an architecture that consists of parts that communicate with each others. The SyllabNet project mentioned in Section 2.1.3 is just an example for this kind of systems. Distributed systems are long studied research topic, it has also spawned the well-known "Open Systems Interconnection" (OSI) model.

The OSI model was defined by both the standardization bodies of the International Standards Organization (ISO [29], which has issued OSI as an International Standard [30]), and ITU-T (the former CCITT, which has issued OSI as Recommendation X.200).

The OSI standard states that

> "...Only the external behaviour of Open Systems is retained as the standard of behaviour of real Open Systems."

This has caused another big area of standardization efforts: What can be done to make someone sure that a "real Open System" indeed conforms to the respective "standard of behaviour"? The answer to this was the development of the "Conformance Testing Methodology and Framework" (CTMF, ISO-9646 [31]).

The CTMF model has various advantages and disadvantages [32, 33, 34, 35, 36]. From the point-of-view of the size and complexity of the ISO-9646 test suites, a particular disadvantage of the CTMF methodology is that the Abstract Test Suite (ATS) developer is required to explicitly classify each possible responses for each test stimulus. This practically means that the "inverse" of the respective protocol specification has to be included in each ATS. This problem was investigated in detail by Russil Wvong in the case of the X.25 protocol [35, 36].

2.2.1 A possible solution for the ISO-9646 ATS complexity problem

Wvong in his X.25 related master's thesis [35, 36] has suggested that it might be advantageous to include trace analysis methods into the conformance testing methodology. Inspired by his work I have suggested [D1, J4, J5, C6] a solution to incorporate SDL based trace analysis in to the CTMF framework. The solution allows the use of trace analysis with only the minimally necessary disruption to the existing methodology.

The key part of the solution is to decompose the ISO-9646 test campaign verdict-making rules into two:

1. An *automated* decision about the validity of the response of the Implementation Under Test (IUT) for a given stimulus with respect to the protocol specification. This decision can be the outcome of some automated trace analysis that requires machine-processable protocol specifications (e.g. in SDL [37]). The use of trace analysis relieves the ATS developer from the error-prone burden of the explicit qualifications of all possible outcomes of the test case.

2. A decision with respect to the expectedness, or unexpectedness of the response from the IUT. This specification can be the main and only content of ATS-es that utilize trace analysis.

These new results are detailed in Section 3.4.

2.3 The problem of satisfiability and big systems

The test generation methods of telecommunication protocols [C4] are often suffers from complexity problems: the bigger the size (complexity) of the protocol specification the faster the (exponential) growth of the size of corresponding ATS [38, 39, 40, 41].

This has turned my attention toward methods and solutions for engineering applications that involve NP-hard optimization problems, in which a heuristic is used to find the optimum or near-optimum of a cost or objective function. There are many approximation techniques aiming to overcome time requirements of exhaustive searches. For a recent review of such approximations see, e.g., [42]. Recently, a novel technique called STAGE using function approximators (FAPPs), e.g., artificial neural networks, and a specific approximation of reinforcement learning (RL, [43]) has been suggested in [15, 44].

STAGE, indeed, showed attractive properties in our studies [J2, C7] on real-world engineering problems.

STAGE has also shown excellent performance on combinatorial problems such as bin-packing, map-coloring, channel routing, etc. [44, 15, 45], but it had some weaknesses, as shown in [C7]. STAGE can often recognize the structure of the state space and make use of this structure to guide the search to better regions of the search space quickly. However, its stability and reliability depends heavily on the used FAPP and the original STAGE algorithm is not a parallel technique.

2.3.1 Combining the algorithms GA and STAGE

Genetic algorithms (GA-s) are well known for their stability and their suitability for parallel implementations. It is also known that they can be combined with local search (LS) techniques to speed up their convergence to the exact global optimum [46, 47, 48, 49]. Liang *et al.* [50, 51] has also developed techniques to combine FAPPs, local searches and evolutionary techniques. Liang's work, however, does suffer from the dimensionality problem and it deals with only continuous problem space.

This has motivated the development of a new algorithm, which combines genetic algorithm (GA) and STAGE. In this version of GA, called GA with Stagenis (GAw-Stagenis, or simply GAS), the fitness of the individuals is determined as the best value found by a local search (LS) starting from the state the individual represents.

New individuals are introduced by the standard crossover operator of GA and by a new genetic operator 'Stagenis' (*i.e.*, STAGE-assisted genesis). Mutation is covered by this Stagenis operation. STAGE makes use a FAPP to approximate and smoothen the objective function. GAS makes use of the same technique. In the Stagenis operation first a LS is executed on the FAPP and then an individual is generated at the minimum of this FAPP.

New scientific results of GAS are published in [J2, J6, C7] and discussed in Section 3.5.

File `Id: glue.tex,v 1.1 2004/11/08 09:45:48 ziegler Exp`

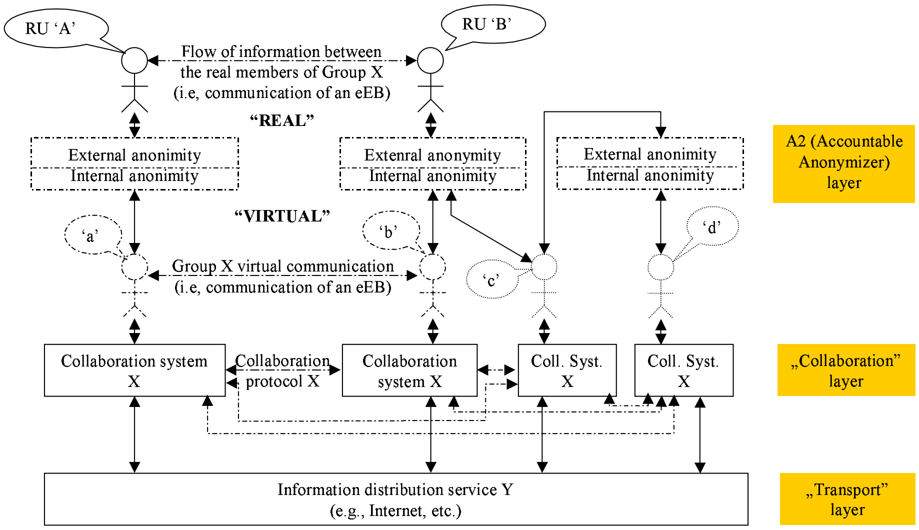

Figure 1: Layered framework for anonymous, but accountable communities.

3 New scientific results

3.1 Anonymous, but accountable communities

Claim-group 1. *I have defined a method, a layered-framework and corresponding communication and security protocols to support anonymous, but accountable communities [J1, C3].*

Claim 1.1. *I have defined a layered-framework [C3] that can support anonymous, but accountable communities, as shown in Figure 1, and further elaborated in [J1], see Figure 2.*

The framework contains three layers, each of them might be sub-divided further:

- The lowest layer is the “communication transport layer”, which provides the basic communication transport service. cooperation of members of the community.

- The “collaboration layer” provides means of cooperation for the community members.

- The “Accountable Anonymizer (A2) layer” supports the protection of sensitive data of the members while it provides means for revealing the protected data in justified cases.

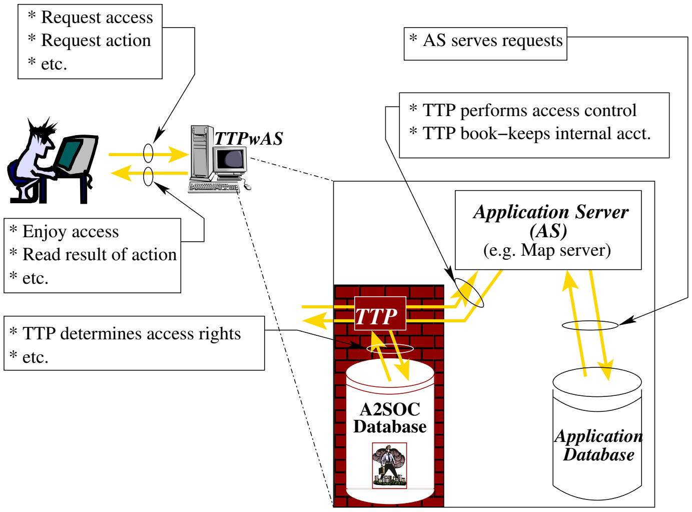

Figure 2: TTP with Application Server (TTPwAS). The TTP acts as a "firewall" between the users and the AS. That is, TTP realizes the Access Control function and maintains the book-keeping of internal accountability.

The communication transport layer can be any networking technology, such as HTTP [52], SMTP [53], or SOAP [54].

The collaboration layer is usually provided by some group-ware application. This can be a typical “forum” software on an Internet portal, or a client-server application, such as a map-server with client map-editors [17].

The definition of an accountable anonymizer service is the main contribution of the thesis Claim-group 1

Claim 1.2. *I have defined a method based on public-key threshold-cryptography. It supports the protection of “secrets” (like personal data, i.e., anonymity) via encryption by the public-key of the “community”. It also makes possible to reveal these secrets in justified cases in a democratic voting procedure (i.e., supporting accountability). The voting process is realized as the threshold-decryption procedure. Each Board Member (BM) holds a fragment of the private-key (a “share”) belonging to the public-key of the community.*

Achieving a “quorum” is defined as reaching the threshold of the cryptosystem. If enough Board Member is willing to apply his/her key-share to the decryption process then it is possible to decrypt, otherwise it is not.

3.1.1 Security protocols

Claim 1.3. *I have defined security and communication protocols for the framework defined in thesis Claim 1. With this I have managed to avoid the requirement of "full-trust" in the A2SOC server in case of verified registration (refer to Thesis 1.3.1).*

Subclaim 1.3.1. *Based on [C3] I have defined [J1] a protocol for verified registration to the A2SOC community via a "trusted A2SOC Authority" (TAA). At the end of the successful execution the user receives a new virtual identity.*

The involvement of the TAA ensures that the A2SOC server does not see the clear-text version of the registration data. The clear-text registration data is verified by the TAA, then it is encrpyted before being sent over to the A2SOC server.This protocol provides the stronger level of accountability (both external and internal).

Subclaim 1.3.2. *Based on [C3] I have defined [J1] a protocol for* non-verified *registration to the A2SOC community. At the end of the successful execution the user receives a new virtual identity. This Protocol is the same as the protocol of Claim 1.3.1. from the point of the view of the user, however, it is different at the server side.*

This provides a somewhat simplified registration procedure, but also the A2SOC server sees the clear-text registration data. The content of the registration data is not verified by the A2SOC server, who is supposed to delete the clear-text registration data after encrypting it.

Subclaim 1.3.3. *Based on [C3] I have defined [J1] a protocol for registering a descendant virtual identity of an already registered user.*

Subclaim 1.3.4. *Based on [C3] I have defined [J1] a protocol for voting about uncovering the real user behind an accused virtual user. It aids a requestor (e.g., a user) to obtain the real identity of some accused user of the community (external accountability).*

Subclaim 1.3.5. *Based on [C3] I have defined [J1] a protocol to provide means for a user who wants to check the registered data about himself/herselfIt can be used to retrieve one's own registration data for checking purposes.*

3.2 Assurance of the Security Protocols

One of the major problem in dynamic, decentralized systems is the maintenance of information that is necessary for security processing. In the proposed system, the mapping ν : *real user* → *base virtual identity* is encrypted with the public key of the A2C community, and the private key is distributed among the Board Members of the community by threshold secret sharing.

In addition to the security protocols, I provided a formal framework to define the concepts in the model and allow me to establish security properties of our model.

Subclaim 1.3.6. *The A2SOC security protocols provide*

1. *internal accountability*
2. *external accountability*

The proof of the theorem follows naturally from the processes enforced by the protocols.

3.3 Applicability of the new results: the SyllabNet project

To test our ideas in practice, a proof-of-concept testbed project was implemented. The testbed is being developed jointly at the Budapest University of Technology and Economics and the Eötvös Loránd University. For the groupware application to be extended by A2SOC principles we have chosen the Coraler Hostess (as the application server (AS)) and the Coraler MapEditor/MapViewer [17] as the client program for the Coraler Hostess). The Coraler system was chosen given its map-based versatility and that it is freely available for academic use.

File `Id: a2soc.tex,v 1.4 2004/11/13 08:47:57 ziegler Exp`

3.4 Trace analysis and conformance testing

Claim-group 2. *I have formally investigated the reasons behind the inherent complexity of ISO-9646 test suites. I have described a possible remedy for this problem by incorporating trace analysis into the ISO-9646 CTMF framework [55]. The solution [D1, J4, J5, C4, C6] provides as much backward-compatibility as possible with the existing CTMF standard.*

3.4.1 The reasons of complexity of the ISO-9646 test suites

It is known from engineering experience (from both my own engineering experience and also from literature, see, e.g., [36, 35]) that ISO-9646 test suites are complex, therefore error-prone to develop.

Claim 2.1. *I have formally investigated [D1] the reasons behind the inherent complexity of ISO-9646 test suites.*

Subclaim 2.1.1. *I have defined the $RTT(i, s)$ (Required Test Trace) that formally describes the ISO-9646 [56]* test purpose *for the i^{th} test requirement belonging to state s of the IUT. It is either linear, or tree-structured event trace containing stimuli-responses sequence(s), as shown in Figure 3. The observability of any trace from $RTT(i, s)$ determines whether the $PASS$ verdict can be issued, or not.*

$$
\begin{array}{rl}
\multicolumn{2}{l}{RTT(i,s) = \{} \\
\mathbf{START}: & (i_1, o_1), (i_2, o_2), \ldots, (i_k, \{o_{k,1} : \mathbf{alt1}, \ldots, o_{k,K} : \mathbf{altK}\}); \\
\mathbf{alt1}: & (i_{\mathrm{alt1},1}/o_{\mathrm{alt1},1}), \ldots, (i_{\mathrm{alt1},l}/\{o_{\mathrm{alt1},l} : \mathbf{altK}, \ldots, o_{\mathrm{alt1},l} : \mathbf{altM}\}) \\
\mathbf{alt2}: & (i_{\mathrm{alt2},1}/o_{\mathrm{alt2},1}), \ldots \\
\ldots: & \\
\mathbf{altN}: & \ldots \\
\mathbf{altZ}: & (i_{\mathrm{altZ},1}/o_{\mathrm{altZ},1}), \ldots, (i_{\mathrm{altZ},M}/o_{\mathrm{altZ},M}) \\
\} &
\end{array}
$$

where

$$\forall i, j : (i = \tau) \Rightarrow (j \neq \tau) \land (j = \tau) \Rightarrow (i \neq \tau)$$

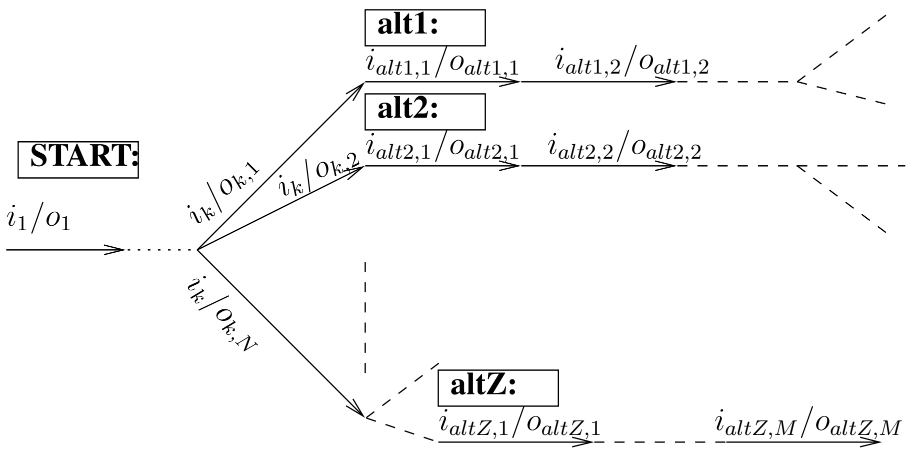

Figure 3: The tree-like RTT required test trace

Subclaim 2.1.2. *I have defined the following $\leq_{prec}$ relation (read precursor-relation) between two input/output event sequences.*

$$\begin{array}{rcl}
\textbf{IF } IO_1 & = & ((i_1/o_1), (i_2/o_2), \ldots, (i_p/o_p)); \\
\textbf{AND } IO_2 & = & IO_1 \cdot ((i_{p+1}/o_{p+1}), (i_{p+2}/o_{p+2}), \ldots, (i_q/o_q)) \\
 & = & ((i_1/o_1), \ldots, (i_p/o_p), (i_{p+1}/o_{p+1}), \ldots, (i_q, o_q)); i_k \in I, o_k \in O, q \geq p, \\
\textbf{THEN} & & IO_1 \leq_{prec} IO_2
\end{array}$$

This relation is non-symmetrical, reflexive *and* transitive.

Informally it means that an event sequence IO_1 of length p is the precursor of another IO_2 of length $q, p \leq q$ if the events (i_j/o_j) from IO_1 are pairwise equivalent with the respective (i'_j/o'_j) from the beginning of IO_j.

Subclaim 2.1.3. *I have defined $RTT_{All}(i, s)$, the set of all possible traversals of $RTT(i, s)$. The members of this set are individual test traces $RTT_j(i, s)$ of length*

*L that each start at the **START** label and ends in a leaf of the test-tree, therefore describes possible test-outcomes (assuming that no test-case error occurs). The size of the set $J = |RTT_{All}(i,s)|$ gives us the number of verdicts that the test case designer should compute for test purpose i of IUT state s:*

$$\begin{aligned} RTT_{All}(i,s) &= \{RTT_j(i,s) \in RTT(i,s) | j = 1,\ldots,J\}, \\ & \quad \text{where} RTT_j(i,s) = ((i_{1,j}/o_{1,j}), (i_{2,j}/o_{2,j}), \ldots, (i_{L,j}/o_{L,j})) \end{aligned}$$

Subclaim 2.1.4. *I have defined the set of all possible precursors of $RTTj(i,s)$ as follows:*

$$\begin{aligned} RTT_j^*(i,s) &= \{IO_{k,j} \leq_{prec} RTT_j(i,s) | k = 1,\ldots,L; \\ & \quad l \leq m \Rightarrow IO_{l,j} \leq_{prec} IO_{m,j}; \\ & \quad l \neq m \Rightarrow IO_{l,j} \neq IO_{m,j}\} \end{aligned}$$

Subclaim 2.1.5. *I have defined the set of all possible alternative traversal $RTT^*(i,s)$ of $RTT(i,s)$ as follows*

$$RTT^*(i,s) = \bigcup_j RTT_j^*(i,s)$$

Subclaim 2.1.6. *I have categorized the possible responses to a given test-stimulus i_k into two classes: the set of expected* acceptable *answers O_k^{acc} and the set of not-expected* unacceptable *answers O_k^{unacc}, which together gives us the set of all possible answers $O_k = O_k^{acc} \cup O_k^{unacc}$ to the k^{th} test-stimulus i_k. Based on this categorization I have classified the possible input/output event pairs at the k^{th} level of $RTT(is)$ into three:*

Expected response *We got this case if the IUT responses to the i_k stimulus with any of the acceptable answers $o_k \in O_k^{acc}$. This means that the observed test trace T_k is in the set of acceptable T_k^{acc} test traces of length k. In other word, the following* *property holds:*

$$T_k = \{T_{k-1} \cdot (i'_k/o'_k) | i'_k = i_k; o'_k \in O_k^{acc}\} \in T^{acc}$$

The size of this set is $|T_k^{acc}| = |O_k^{acc}|$. This size is the same as that of $RTT_k(i, s)$.

Unexpected response *We got this case if the IUT responses to the i_k stimulus with any of the unacceptable answers, that is, $o_k = o_e \notin O_k^{acc}$. This means that the observed test trace T_k is not in the set of acceptable T_k^{acc} test traces of length k. This case also may produce more than one unacceptable responses, there fore it is a set: T^{unacc}. The following property holds:*

$$T_k = \{T_{k-1} \cdot (i'_k/o'_k) | i'_k = i_k; o'_k \in O_k^{unacc}\} \in T^{unacc}$$

The size of this set is $|T_k^{unacc}| = |O| - |O_k^{acc}|$

Response without a stimulus *It is possible in certain cases that before sending the $i_k \neq \tau$ (τ is the empty event) stimulus the IUT sends some $o' = o_k \neq \tau$, which means that an implicit $i'_k = \tau$ must be inserted into the test trace T_k, since that must hold event-pairs. These outcomes also make a set: TT_k^{unacc}. The following property holds:*

$$T_k = \{T_{k-1} \cdot (i'_k/o'_k) | i'_k = \tau; o'_k \in O\} \in TT^{unacc}$$

Since the number of unexpected messages equals to the size of the output alphabet O, therefore the size of this set is $|TT_k^{unacc}| = |O|$

This means that we can assign a preliminary $PASS$verdict for the branches equaling to T_k^{acc}, but cannot assign verdict for the cases of $T_k^{unacc} \cup T_k^{unacc}$. This latter needs either $FAIL$, or maybe $INCONCLUSIVE$verdicts. These latter verdicts cause the most difficulties for test case designers and cause most of the complexity.

Subclaim 2.1.7. *I have shown that the ISO-9646 CTMF requirement of explicit categorization of all possible outcomes makes the branching factor considerably bigger:*

at step k instead of the minimally necessary $|O_k^{acc}| = |RTT_k(i,s)|$, often considerably more responses should be taken into account:

$$|O_k^{acc}| + (|O| - |O_k^{acc}|) + |O| = 2 \cdot |O|$$

Claim 2.2. *Based on the notion of $RTT(i,s)$ Required Test Trace for test purpose i in state s and on the notion of the particular j^{th} depth-first traversal $RTT_j(i,s)$ of $RTT(i,s)$, I have formally defined the complete Test Case $TC(i,s) = \bigcup_j TC_j(i,s)$ that contains the classifications (verdicts) of all possible events.*

$$\begin{array}{rcl}
TC_j(i,s) & = & \{(T_{k,j}, VERDICT) | k = 1,2,\ldots,L; j = 1,2,\ldots \leq 2 \cdot |O|\} \\
\text{where} & & T_{k,j} \in T_k^{acc} \cup T_k^{unacc} \cup TT_k^{unacc} \\
\text{and} & & L_j = |RTT_j(i,s)| \\
\text{and} & & RTT_j(i,s) \leq_{prec} RTT(i,s) \\
\text{and} & & T_k^{acc} \in RTT_j^*(i,s) \\
\text{and} & & VERDICT \in \{PASS, FAIL, INCONCLUSIVE\} \\
\text{furthermore} & & [T_{k,j} \in T_k^{acc} \in RTT_j^*(i,s) \Leftrightarrow T_{k,j} \leq_{prec} RTT_j(i,s)] \\
 & & \Rightarrow VERDICT = PASS \\
\text{and} & & [T_{k,i} \in T_k^{unacc} \cup TT_k^{unacc}] \Rightarrow VERDICT \neq PASS \\
TC(i,s) & = & \bigcup_j TC_j(i,s)
\end{array}$$

It is a well-known empirical fact among test-engineers that in practical cases $|O^{acc}| \ll 2 \cdot |O|$. Indeed, handling of unforeseen, unexpected test cases is arguably the biggest difficulty that a test-suite designer must face. This challenge often defeats [36, 35] even the test-suite designers of highly-respected standardization bodies, like ETSI [12], or ITU [9].

3.4.2 Applying trace analysis to the ISO-9646 CTFM

I have suggested the partial re-definition of the ISO-9646 Conformance Testing Methodology and Framework (CTMF) [31, 56, 57, 58, 59] to ease the burden of handling unexpected and unforeseen events during test suite design.

Claim 2.3. *I have decomposed the original monolithic verdict-making mechanism of ISO-9646 into two related, but independent verdict making mechanisms: a decision about the test purpose observability and a decision about possible behavioral violations of the protocol specification, as shown in Table 1. In order to make this possible I have also decomposed the ISO-9646 "tester" into two: a test-driver and a trace-analyzer, as shown in Figure 4.*

The original ISO-9646 "tester" fulfills two roles: first is to control the test-campaign and second is to observe and analyze the responses.

Subclaim 2.3.1. *I have decomposed the ISO-9646 "tester" entity into the following two entities while I preserved as much backward compatibility with the previous test architecture as possible:*

The test driver *is responsible for controlling the test campaign. It has only a very limited "go — no go" analyzer role with respect to the set of possible responses. If the response is expected ("go") then it proceeds with the test campaign for test purpose i of state s, according to $RTT(i, s)$. If the response is not expected ("no go") then it consult with its dual entity, the trace analyzer.*

The trace analyzer *is responsible for monitoring and analyzing the test campaign. From this point-of-view it is a passive entity. It tries to match the observed input-output events with the set of all permitted traces from the specification and reports the failure, of the success of this attempt.*

This dual-entity replacement of the ISO-9646 "tester" is shown in Figure 4.

File `Id: traceconf.tex,v 1.3 2004/11/13 08:47:57 ziegler Exp`

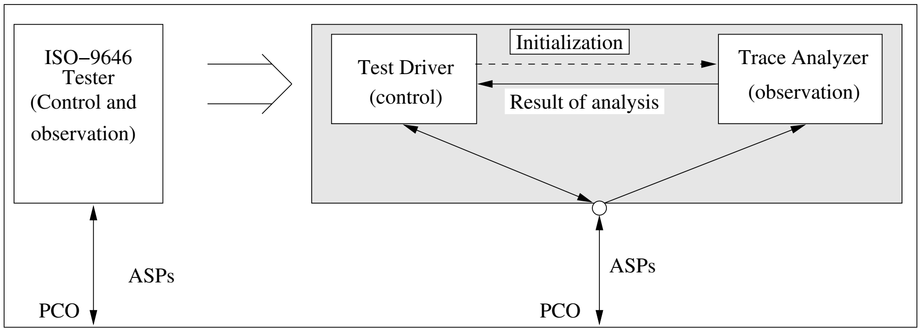

Figure 4: Replacement of the ISO-9646 Tester with Test Driver and Trace Analyzer

The decision of the trace analyzer about the observed events during the test	The decision of the test driver about the observability of of the $RTT(i, s)$	The VERDICT according to ISO-9646
there *was* an error	*(in this case irrelevant)*	$FAIL$
there *was no* error	*was* successful	$PASS$
there *was no* error	*was not* successful	$INCONCLUSIVE$

Table 1: Decomposition of the ISO-9646 verdict making mechanism

3.5 Stagenis

Claim-group 3. *I have investigated the possibilities of combining the Stage [15, 44, 45] algorithm and the Genetic Algorithms (GA) [60]. I have suggested a three-levels memory approach, which resulted in the the GA-with-Stagenis, or shortly GAS algorithm.*

Claim 3.1. *I have suggested to combine Stage and Local Search (LS) boosted GA (LS-GA) algorithms [46, 47, 48].*

The combination makes possible to retrain the Function Approximator (FAPP) of Stage from the search trajectories of those LS runs of LS-GA that are used to calculate fitness values of GA population members.

Claim 3.2. *I have defined a new GA operator called Stage-Assisted-Genesis, or shortly Stagenis. This new operator can be used as a special form of mutation operator besides the other traditional GA operators of recombination and selection.*

The Stagenis operator uses the training data of the Stage-FAPP to "create" new members for the population. This "creation" is obtained by performing a local search in the "feature-space" of problem that is approximated by the FAPP similarly to the philosophy of the original Stage algorithm [15, 45, 44]. This constitutes a three-level memory:

1. The trajectory of the LS forms the short term memory.
2. Parameters of the function approximator of STAGE make the medium-term memory, which aims to uncover the underlying global structure of the search problem.
3. The population of the GA is the long-term memory, which stabilizes and selects local minima and/or schemas of those structures against the biased search of STAGE.

The GAS Algorithm is defined by the following pseudo code:

Claim 3.3. *I have made simulation experiments to evaluate the performance of the GAS algorithm. I have found that while GAS is generally not faster than Stage (on*

Algorithm 1 The GAS algorithm in pseudo-code

```
PROCEDURE LS.optimize($x$)
   RETURN the best $Obj$ found by a LS starting from $x$
END

PROCEDURE FLS.optimize($x$)
   RETURN the best state found by a FLS starting from $x$
END

INITIALIZE $old\_population$
   with $population\_size \cdot (1 - stagenis\_rate)$ random $x_i$ members
FOR EACH $x_i \in old\_population$ $Fitness(x_i) = LS.optimize(x_i)$
   LOAD trajectory $i$ into FAPP
FOR $i = 1$ TO $population\_size \cdot stagenis\_rate$
   SET $x_i = FLS.optimize(randomstate)$
   INSERT $x_i$ in $old\_population$
   $Fitness(x_i) = LS.optimize(x_i)$
   LOAD trajectory $i$ into FAPP
REPEAT
   FOR $i = 1$ TO $population\_size \cdot$ $(stagenis\_rate + 2 \cdot recombination\_rate)$
      IF $i \equiv 0 \mod (\lfloor \frac{population\_size \cdot (stagenis\_rate + 2 \cdot recombination\_rate)}{population\_size \cdot stagenis\_rate} \rfloor)$
      THEN
         $x_i = FLS.optimize(randomstate)$
         INSERT $x_i$ in $new\_population$
         $Fitness(x_i) = LS.optimize(x_i)$
         LOAD trajectory $i$ into FAPP
      ELSE
         SELECT $(x_i, x_j)$ of $old\_population$ with
            selection likelihood proportional to $Fitness(\cdot)$
         SET $(x'_i, x'_j) = recombinate(x_i, x_j)$
         INSERT $(x'_i, x'_j)$ into $new\_population$
         $Fitness(x'_i) = LS.optimize(x'_i)$
         $Fitness(x'_j) = LS.optimize(x'_j)$
         LOAD both trajectories into FAPP
         INCREMENT i //recomb. generates 2 new members!
         FI
      FILL_UP the rest of $new\_population$
          with the best members of $old\_population$
          according to their fitness
      FOR EACH such member retain the old $Fitness(\cdot)$
   UNTIL <#Gens|#LS|#Evals> exceeds <MaxGens|MaxLS|MaxEvals>
RETURN the best state ever found during LS runs.
```

single processor machines) the Stagenis operator boosts GA making it comparable to Stage. Furthermore, GAS is suitable for parallelization, contrary to the original Stage.

Considering that Stage is inherently a sequentially iterating algorithm GAS promises us the possibility of almost linear speed-up, as shown by Mann and Orbán in [J6].

File `Id: stagenis.tex,v 1.3 2004/11/13 08:47:57 ziegler Exp`

4 Acknowledgement

First of all I would like to thank my previous and current supervisors (in temporal order): Dr. János Miskolczi, Dr. András Lőrincz and Dr. Csilla Farkas. Their support was invaluable.

It would have been impossible to finish my Ph.D. ever, without the strong support of my host institution, the Department of Telecommunication and Media Informatics at Budapest University of Technology and Economics. I wish to thank all of my colleagues here, but especially my boss, Dr. Tamás Henk and the former and current heads of the department: Professor Dr. Géza Gordos and Professor Dr. Gyula Sallai.

I owe thanks to all industrial, governmental and non-governmental grants and stipends that supported directly, or indirectly (parts) of my works. The most prominent ones are: Ericsson Hungary, Matáv PKI, the Hungarian Ministry of Informatics and Telecommunication, the Hungarian Ministry of Education and the Pro-Progressio Foundation.

Last, but not least my thanks should go to my family:...

File `Id: ack.tex,v 1.3 2004/11/13 08:47:57 ziegler Exp`

References

[1] Gary C. Kessler. *ISDN – second edition*. McGraw-Hill Series on Computer Communications. McGraw-Hill, 1995.

[2] John G. van Bosse. *Signalling in Telecommunication Networks*. John Wiley & Sons, Inc., 1998.

[3] Bartucz János and Horváth Tamás. *Az ISDN alapjai*. Puskás Tivadar Távközlési Technikum, 1996. In Hungarian.

[4] Gunnar Heine. *GSM Networks: Protocols, Terminology, and Implementation*. Artech House Mobile Communications Library. Artech House, Boston–London, 1999.

[5] The UUCP project. http://www.uucp.org/.

[6] What is the internet? definitions on the web. http://www.google.com/search?q=define:Internet.

[7] Voice on the net–VON. http://www.von.com/.

[8] Imt-2000 activities of the itu. http://www.itu.int/home/imt.html.

[9] ITU-T–itu telecommunication standardization sector. http://www.itu.int/ITU-T.

[10] Ralf Kreher, Juergen Placht, and Torsten Ruedebusch. *UMTS UTRAN Signalling*. Tektronix Network Diagnostics Academy. Pro BUSINESS Gmbh, Berlin, 2003.

[11] The 3rd generation partnership project (3GPP). http://www.3gpp.org/.

[12] ETSI–european standards institute. http://www.etsi.org/.

[13] International standard ISO 7498-1984 (e): Information technology – open systems interconnection – reference model – part 1: Basic reference model.

[14] T. Csöndes, S. Dibuz, and B. Kotnyek. Test suite reduction in conformance testing. *Acta Cybernetica*, Vol. 14.(No. 2.):229–238, 1999.

[15] J. A. Boyan. *Learning Evaluation Functions for Global Optimization*. PhD dissertation, School of Computer Science, Carnegie Mellon University, Pittsburgh PA 15213, August 1998. Available on-line at http://www.ri.cmu.edu/pubs/pub_2954.html.

[16] C. Reeves and C. Höhn. Integrating local search into genetic algorithms. In V.J.Rayward-Smith, I.H.Osman, C.R.Reeves, and G.D.Smith, editors, *Modern Heuristic Search Methods*, pages 99–115. John Wiley & Sons, New York, 1996.

[17] The SyllabNet project. http://syllabnet.tmit.bme.hu.

[18] P. F. Syverson amd D. M. Goldschlag and M. G. Reed. Anonymous connections and onion routing. In *Proc. IEEE Symposium on Security and Privacy, Oakland, California*, 1997.

[19] M. K. Reiter and A. D. Rubin. Crowds: anonymity for web transactions. *ACM Transactions on Information and System Security*, 1(1):66–92, 1998.

[20] C. Shields and B. N. Levine. A protocol for anonymous communication over the internet. In *Proc. of ACM Conference on Computer and Communications Security*, 2000.

[21] K. Bennett, C.Grothoff, T. Horozov, I. Patrascu, and T. Stef. Gnunet — a truly anonymous networking infrastructure. http://citeseer.nj.nec.com/502472.html.

[22] Ian Clarke, Oskar Sandberg, Brandon Wiley, and Theodore W. Hong. Freenet: A distributed anonymous information storage and retrieval system. volume 2009, pages 46+. Springer, 2001.

[23] Napster. http://www.napster.com/about_us.html, 2002.

[24] D. L. Chaum. Untraceable electronic mail, return addresses and digital pseudonyms. *Communications of ACM*, 24(2), 1981.

[25] I. Goldberg, D. Wagner, and E. Brewer. Privacy-enhancing technologies for the internet. In *Proc. of 42nd IEEE Spring COMPCON*, 1997.

[26] J. Claessens, B. Preneel, and J. Vandewalle. Anonymity controlled electronic payment systems. In *Proc. 20th Symp. on Information Theory in the Benelux*, 1999.

[27] P. MacKenzie and J. Sorensen. Anonymous investing: Hiding the identities of stockholders. In *Proceedings of Financial Crypto '99*, volume 1648 of *Lecture Notes in Computer Science*, 1999.

[28] D. Kugler and H. Vogt. Off-line payments with auditable tracing. In *Financial Cryptography*, Lecture Notes in Computer Science. Springer-Verlag, 2002.

[29] ISO–International Organization for Standardization. http://www.iso.org.

[30] Draft international standard ISO/IEC DIS 7498-1 (CCITT Rec. x.200): Information technology – open systems interconnection – reference model – part 1: Basic reference model, revison of first edition, 1993.

[31] Final draft international standard ISO/IEC 9646-1: 1994(e): Information technology – open systems interconnection – conformance testing methodology and framework: – part 1: General concepts, 14 March 1994.

[32] B. S. Bosik and M. Ü. Uyar. Finite state machine based formal methods in protocol conformance testing: from theory to implementation. *Computer Networks and ISDN Systems*, (22):7–33, 1991.

[33] D. P. Sidhu and T. Leung. Formal methods for protocol testing: A detailed study. *IEEE. Trans. on Softw. Eng.*, 15(4):413–426, April 4 1989.

[34] Jinsong Zhu and Samuel T. Chanson. Towards evaluating fault coverage of protocol test sequences. In *PSTV'94. The 14th International IFIP Symposium on Protocl Specification, Testing & Verification*, Vancouver, B.C. Canada, 7-10 June 1994.

[35] R. Wvong. LAPB conformance testing using trace analysis. In *11th Int'l Symposium on Protocol Specification, Testing, and Verification*, pages 248–261, June 1991.

[36] Russil Wvong. A new methodology for OSI conformance testing based on trace analysis. Master's thesis, University of British Columbia, Oct 1990.

[37] Ove Fargemand and Anders Olsen. *Introduction to SDL-92*. TFL Telecommunications Research Laboratory, Lyngso Allé 2, DK-2970 Horsholm, Denmark, July 27 1992.

[38] Hasan Ural and Keqin Zhu. Optimal length test sequence generation using distinguishing sequences. *IEEE Transactions on Networking*, 1(3):358–371, June 1993.

[39] Fumiako Sato and Tadanori Mizuno. An optimized test sequence generation method for communication sytems — improved sw method. *Special Issue on Communication Software Technologies, IEICE Trans. Commun.*, E75-B(10):1024–1031., October 1992.

[40] A. V. Aho, A. T. Dahbura, D. Lee, and M. U. Uyar. An optimization technique for protocol conformance test generation based on uio sequences and rural chinese postman tours. In S. Aggarwal and K. Sabnani, editors, *Proc. 8th Int. Symp. on Protocol Specification, Testing and Verification*, pages 75–86. North Holland, 1988.

[41] M. Ü. Üyar and A. T. Dabhura. Optimal test sequence generation for protocols: the chinese postman algorithm applied to q.931. In *Proc. of IEEE Global Telecommunication Conference*, volume 1 of 3, pages 68–72, Houston, Tx., USA, 1–4th December 1986.

[42] D.S. Hochbaum, editor. *Approximation Algorithms for NP-Hard Problems*. PWS Publishing Co., Boston, 1995.

[43] R. S. Sutton and A. G. Barto. *Reinforcement learning: An introduction*. MIT Pess, 1998.

[44] J. A. Boyan and A. W. Moore. Learning evaluation functions to improve optimization by local search. *Journal of Machine Learning Research*, 1:77–122, November 2000.

[45] J. A. Boyan and A. W. Moore. Learning evaluation function for global optimization and boolean satisfiability. In *Proceedings of the Fifteenth National Conference on Artificial Intelligence (AAAI)*, page 14, 1998.

[46] N.L.J. Ulder, E.H.L. Aarts, H.J. Bandelt, P.J.M. van Laarhoven, and E. Pesch. Genetic local search algorithms for the travelling salesman problem. In *First International Conference on Parallel Problem Solving from Nature PPSN*, pages 109–116, 1990.

[47] Thomas Kammeyer and R. K. Belew. Stochastic context-free grammar induction with a genetic algorithm using local search. In Richard K. Belew and Michael Vose, editors, *Foundations of Genetic Algorithms IV*, University of San Diego, CA, USA, 3–5 1996. Morgan Kaufmann.

[48] B. Freisleben and P. Merz. Genetic local search for the TSP: New results. In *Proceedings of The IEEE International Conference on Evolutionary Computation*, pages 159–164. IEEE Press, 1997.

[49] R. Dorne and J.K. Hao. A new genetic local search algorithm for graph coloring. In A.E. Eiben, T. Bäck, M. Schoenauer, and H.P. Schwefel, editors, *Parallel Problem Solving from Nature – PPSN V*, Lecture Notes in Computer Science 1498, pages 745–754, Berlin, 1998. Springer-Verlag.

[50] Ko-Hsin Liang, Xin Yao, and Charles Newton. Evolutionary search of approximated n-dimensional landscapes. *International Journal of Knowledge-Based Intelligent Engineering Systems*, 4(3):172–183, July 2000.

[51] Ko-Hsin Liang, Xin Yao, and Charles Newton. Combining landscape approximation and local search in global optimization. In Peter J. Angeline, Zbyszek Michalewicz, Marc Schoenauer, Xin Yao, and Ali Zalzala, editors, *Proceed-*

ings of the Congress on Evolutionary Computation, volume 2, pages 1514–1520, Mayflower Hotel, Washington D.C., USA, 6-9 1999. IEEE Press.

[52] IETF – The Internet Engineering Task Force. RFC 2616 – The Hypertext Transfer Protocol (HTTP). http://www.ietf.org/rfc/rfc2616.txt.

[53] IETF – The Internet Engineering Task Force. RFC 2821 – Simple Mail Transfer Protocol. http://www.ietf.org/rfc/rfc2821.txt.

[54] W3C – World-Wide-Web Consortium. Simple Object Access Protocol (SOAP). http://www.w3.org/TR/soap/.

[55] International standard ISO/IEC 9646-1: Information technology – open systems interconnection – conformance testing methodology and framework: – part 1: General concepts.

[56] Final draft international standard ISO/IEC 9646-2: 1994(e): Information technology – open systems interconnection – conformance testing methodology and framework: – part 2: Abstract test suite specification, 14 March 1994.

[57] International standard ISO/IEC 9646-3: 1992(e): Information technology – open systems interconnection – conformance testing methodology and framework: – part 3: The tree and tabular combined notation (TTCN). first edition, 1 October 1992.

[58] Final draft international standard ISO/IEC 9646-4: 1994(e): Information technology – open systems interconnection – conformance testing methodology and framework: – part 4: Test realization., 14 March 1994.

[59] Final draft international standard ISO/IEC 9646-5: 1994(e): Information technology – open systems interconnection – conformance testing methodology and framework: – part 5: Requirements on test laboratories and clients for the confromance assessment process, 14 March 1994.

[60] Jörg Heitkötter and David Beasley (editors). The Hitch-Hiker's Guide to Evolutionary Computation (FAQ in comp.ai.genetic). http://www.cs.cmu.edu/Groups/AI/html/faqs/ai/genetic/top.html, Aug 1997.

Publications of New Results

[D] **Dr.univ theses**

[D1] **G. Ziegler**. *Protokollok konformancia tesztelése eseményelemző módszerrel (Protocol conformance testing using trace analysis).* University doctor's thesis, Technical University of Budapest, 1996. (In Hungarian.).

[J] **Journal articles**

[J1] **G. Ziegler**, C. Farkas, and A. Lőrincz. A framework for anonymous but accountable self-organizing communities. *Information and Software Technology*, 2004. Submitted manuscript.

[J2] Zs. Palotai, T. Kandár, Z. Mohr, T. Visegrády, **G. Ziegler**, P. Arató, and A. Lőrincz. Value prediction in the allocation problem of high level synthesis with IP-s. *Journal on Applied Artifical Intelligence*, 16(2):117–157, February 2002.

[J3] M. Törő and **G. Ziegler**. Validation of abstract test suites with use of SDL. *Microprocessing and Microprogramming*, (40):711–714, 1994.

[J4] Gy. Vesztergombi and **G. Ziegler**. SDL alapú protokollok elemzése (Analysing SDL based protocols). *Híradástechnika (Journal on Telecommunications)*, L(8):26–25, August 1999. (In Hungarian).

[J5] **G. Ziegler** and J. Miskolczi. Új módszerek a protokoll alkalmasság vizsgálatban: nyomelemzés. *Híradástechnika (Journal on Telecommunications)*, XLVII(8):47–52, June–July 1996. (In Hungarian).

[J6] **G. Ziegler**, Z. Á.Mann, A. Orbán, Zs. Palotai, L. Grad and A. Lőrincz. Three-level Memory for Optimization *Applied Soft Computing*, 2003. Submitted.

[C] **Conference articles**

[C1] Zs. Boja-Harangozó, Ta Manh Dung, and **G. Ziegler**. PROCONSUL, a tool for protocol engineering. In A. Pataricza, E. Selényi, and A. Somogyi, editors, *Proceedings of The Eight Symposium on Microcomputer and Microprocessor Applications*, pages 751–759, Budapest, Hungary.

[C2] S. Dibuz and **G. Ziegler**. Protokollok vizsgálata egy új kommunikációs korszak küszöbén. In *VII. Országos Neumann Kongresszus*, Eger, Hungary, June 21-23rd. 2000. NJSZT. CD-ROM, see also: http://www.njszt.hu/neukong/CD_eload_tartj.htm.

[C3] C. Farkas, **G. Ziegler**, A. Meretei, and A. Lőrincz. Supervison of anonymous and accountable self-organizing communities. In S. De Capitani di Vimercati and Pierangela Samarati, editors, *Proceedings of the Workshop on Privacy in the Electronic Society*, pages 81–91. ACM SIGSAC, ACM, November 21 2002. Paper no. 136.

[C4] **G. Ziegler**. Overview of FSM based protocol test sequence generation methods. In A. Pataricza, E. Selényi, and A. Somogyi, editors, *Proceedings of The Eight Symposium on Microcomputer and Microprocessor Applications*, pages 698–707, Budapest, Hungary.

[C5] **G. Ziegler**. Parametrized design of a parallel convolver: algorithm, architecture and circuits. Technical Report 93.124, Delft University of Technology, Department of Electric Engineering, Network Theory Section, Delft, The Netherlands., 1993.

[C6] **G. Ziegler** and J. Miskolczi. Trace analysis method. Technical Report KFKI-1996-07/M, Hungarian Academy of Scienses, Central Research Inistitute for Physics, 1996.

[C7] **G. Ziegler**, Zs. Palotai, T. Cinkler, P. Arató, and A. Lőrincz. Value prediction in engineering applications. In L. Monostori, J. Váncza, and M. Ali, editors, *Engineering of Intelligent Systems, Proceedings of AIE/IEA 2001, Budapest, Hungary*, Lecture Notes in Artificial Intelligence (LNAI) 2070, pages 25–34. Springer, June 4–7 2001.

File `Id: thesis.tex,v 1.2 2004/11/08 09:45:49 ziegler Exp`