JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

2/2011

(Contents Continued on Back Cover)

Editorial Board

Editorial Advisory Board

ISSN 1509-4553 on-line: ISSN 1899-8852

Circulation: 300 copies

Sowa – Druk na życzenie, www.sowadruk.pl, tel. 22 431-81-40

JOURNAL OF TELECOMMUNICATIONS AND INFORMATION TECHNOLOGY

Preface

Studies on the IPv6 protocol began in the early 1990s in The Internet Engineering Task Force (IETF). One of the main reasons for initiating this work at the standardization body was a prediction on accelerated IPv4 address space consumption in the near future and limited free address space available for new allocations. Current forecasts on the IPv4 address exhaustion made by the Internet Assigned Numbers Authority (IANA) indicate that these addresses will run out in May 2011 (http://inetcore.com/project/ipv4ec/index_en.html).

The use of the IP protocol in new application areas, such as mobile phones or the Internet of Things has forced increased budget and efforts on the development of the IPv6 protocol and services and applications associated with it. At the same time, work on acceleration of migration processes, implementation of IPv6 in telecommunication operators' networks and end-user operating systems was intensified.

Transformation from IPv4 into IPv6 is one of short-term aims to be achieved in Europe. To accelerate this process in Poland, we have devoted one of work packages of a national project entitled Future Internet Engineering project (http://www.iip.net.pl/) to recommend best practices and to develop a set of tools supporting this transformation. The partners involved in this work package are from the following organizations: Poznań Supercomputing and Networking Center, Gdańsk University of Technology, National Institute of Telecommunications in Warsaw, AGH University of Technology, Wrocław University of Technology and Warsaw University of Technology.

This issue of the *Journal of Telecommunications and Information Technology*, **edited by Artur Binczewski, Wojciech Burakowski and Józef Woźniak as Guest Editors**, contains four papers related to this project as well as paper written by S. Kukliński, P. Radziszewski and J. Wytrębowicz, focused on the development of the IPv6 technology and practical results achieved.

The first paper, *Why is IPv6 Deployment Important for the Internet Evolution?* by J. Mongay Batalla, A. Binczewski, W. Burakowski, K. Chudzik, B. Gajda, M. Gajewski, A. Grzech, P. Krawiec, J. Kwiatkowski, T. Mrugalski, K. Nowicki, W. Procyk, K. Sienkiewicz, R. Szuman, J. Śliwiński, J. Światowiak, P. Wiśniewski, and J. Woźniak, covers the issue of replacing the IPv4 protocol with IPv6 in the Internet as one of the aims of the European Union policy. The main reason for this replacement is the IPv4 address space exhaustion, which can cause serious complications in the evolution of the Internet and its adoptation in new

areas, e.g., in next generation mobile telephony or so called Internet of Things. Simultaneously, the addressing capabilities of the IPv6 protocol are practically unlimited and its new functionalities increase the attractiveness of its usage. The article discusses problems related to IPv6 deployment in the regular Internet. Especially, the rules for IPv6 deployment and for cooperation of IPv4 with IPv6 (including cooperation tests) at both network and application levels are presented. Moreover, the European projects' results and the activity's directions of the national project "Future Internet Engineering" are discussed.

The second paper, *Iv6 Virtualization Environments* by K. Chudzik and J. Kwiatkowski, provides a short overview of the key features of IPv6 and discusses the possible levels of network virtualization. The research environment for testing the level of support for IPv6 protocol by virtualization environments is proposed. The results of tests conducted using the proposed research environment for Hyper-V virtualizer are presented.

The paper *IPv6 in Wireless Networks* by S. Kukliński, P. Radziszewski and J. Wytrębowicz presents problems related to the construction of autonomous wireless networks based on the IPv6 protocol. Prospects of implementation of IPv6 in wireless networks and IPv6 features and mechanisms important in such applications are discussed, together with an outline of potential research directions for the use of IPv6 in wireless networks. The selected concepts are described in detail, arising from the course of the EFIPSANS project. Concepts presented in the paper apply to wireless ad hoc mesh networks. Their nature and aspects related to their auto-configuration and autonomously operating routing are discussed, with particular focus on wireless autonomic routing framework (WARF).

In the paper *On Implementing IPTV Platform with IPv4 and IPv6 Devices* by J. Mongay Batalla and P. Krawiec, a global solution for integrating all devices, these working on the IPv4 protocol stack and these IPv6-enabled, under the same IPTV platform is proposed. This solution allows end users to receive IPTV streams irrespectively of the IP protocol used. The proposed solution is especially relevant for small IPTV systems, which step by step are progressing towards IPv6.

The last paper devoted to IPv6 technology, *On Testing IPv6 in Small ISP's Networks* by K. Sienkiewicz, M. Gajewski and J. Mongay Batalla, proposes a new approach to IPv6 tests with the particular focus on supporting the IPv6 deployment in small networks. It presents tools and speci?cations for IPv6 tests and proposes a test platform tailored to needs of small ISPs. The test platform is a dedicated LiveCD distribution based on FreeBSD operating system with the IPv6 test environment and a set of prede?ned tests. This solution allows to launch the test tool software on any computer equipped with an Ethernet card and a CD-ROM/DVD-ROM drive. The LiveCD test tool allows users to execute tests and analyzes the results in the graphical environment. Authors believe that this approach will help to simplify and shorten IPv6 testing in small ISP's networks.

Another paper devoted to IP networks is *Dynamic Contracting of IP Services – System Architecture and Prototype* by Piotr Arabas and Mariusz Kamola, dealing with dynamic contracting of IP services, presenting a reservation system which serves requests issued by users demanding setting up network service of specified parameters (QoS). DiffServ technology together with traffic engineering and admission control are used. While similar solutions were developed previously, they failed to find acceptance with network operators. Implementation details and promising results of tests on prototype system set up in NASK laboratory are described. Necessary extensions and possibility of commercialization of such a system are discussed.

D. M. S. Sultan and Md. Taslim Arefin in the paper *GPON, the Ultimate Pertinent of Next Generation Triple-play Bandwidth Resolution* deal with next generation access (NGA) infrastructure, as optical fibers are becoming necessary to satisfy rising demand for bandwidth and reliability, created by services like IP television (IPTV) and video on demand (VoD). While the latest xDSL solutions (i.e., VDSL/VDSL2+, SHDSL) can satisfy bandwidth needs, transmission distance is severely restricted; high bandwidth and long reach can be combined only in a fiber to the home (FTTH) network. One way is to install a passive optical network (PON); of those, Gigabit PON (GPON) is the most advanced PON solution used by European and US providers, while providers in Asia predominantly use EPON/GePON variants. The paper provides overview of GPON network – its architecture, mechanisms and key services.

The article *Developing a Secure Image Steganographic System Using TPVD Adaptive LSB Matching Revisited Algorithm for Maximizing the Embedding Rate*, by P. Mohan Kumar and K. L. Shanmuganathan presents work on hiding a secret message in a variety of multimedia carriers like images, audio or video files. Multiple steganographic algorithms have been proposed and development of steganalytic tools to detect them has progressed, too. This paper concentrates on integrating Tri-way pixel value differencing approach and LSB matching in a new way. The secret data embedded in images were images, text and audio signals so far. The proposed scheme has also come with the executable file as secret data. Experiments shown that necessary properties of steganographic system such as imperceptibility, capacity and resistance against steganalytic tools have been achieved.

The last three papers in this issue are devoted to different issues in radio networks. Multimedia services often have to deal with poor transmission quality, especially to portable devices. In their paper *An Efficient Chaotic Interleaver for Image Transmission over IEEE 802.15.4 Zigbee Network*, Mohsen A. M. M. El-Bendary, Atef Abou El-Azm, Nawal El-Fishawy, Farid S. M. Al-Hosarey, Mostafa A. R. Eltokhy, Fathi E. Abd El-Samie, and H. B. Kazemian present study on transmission of images over IEEE ZigBee 802.15.4, a short-range wireless network, that could be used for multimedia transmissions. The ZigBee network is a wireless personal area network (WPAN), which needs a strong interleaving mechanism for protection against error bursts. A novel chaotic interleaving scheme for this purpose is proposed, utilizing the chaotic Baker map. A comparison study between the proposed chaotic interleaving scheme and the traditional block and convolutional interleaving schemes for image transmission over a correlated fading channel is presented, demonstrating the superiority of chaotic interleaving scheme over the traditional approach.

The next contribution, *Higher Order Cumulants for Identification and Equalization of Multicarrier Spreading Spectrum Systems* by Said Safi, Miloud Frikel, Abdelouhab Zeroual, and Mohammed M'Saad, describes two blind algorithms for multicarrier code division multiple access (MC-CDMA) system equalization. In order to identify, blindly, the impulse response of two practical selective frequency fading channels called broadband radio access network (BRAN A and BRAN E) normalized for MC-CDMA systems, higher order cumulants (HOC) were used to build accurate simulation algorithms. Simulation results for different signal to noise ratios (SNR) successfully demonstrated that the proposed algorithms are able to estimate the impulse response of these channels blindly (without any information about the input), except that the input excitation is identically and independent distributed and non-Gaussian. In the MC-CDMA part, a zero forcing and the minimum mean square error equalizers were used.

Performance of microwave and satellite networks can be significantly degraded by rain-induced attenuation, and the last paper *Characteristics of Measured Rainfall Rate at Ogbomoso, Nigeria for Microwave Applications* by F. A. Semire and T. I. Raji presents characteristics of rainfall rate useful in estimation of attenuation due to rain, based on data collected between January and October, 2009. Result shows that power law relationship exists between the equiprobable rain rates of two different integration times. The value of conversion factor CE and CR obtained for Ogbomoso are 0.28(60) and 0.64(90) respectively. The results show that different conversion factor is required for different location, even within the same climatic region.

We hope the Readers will find this issue of the *Journal of Telecommunications and Information Technology* useful and interesting.

Paweł Szczepański
Editor-in Chief

Paper

Why is IPv6 Deployment Important for the Internet Evolution?

Jordi Mongay Batalla[a], Artur Binczewski[b], Wojciech Burakowski[c], Krzysztof Chudzik[d], Bartosz Gajda[b], Mariusz Gajewski[a], Adam Grzech[d], Piotr Krawiec[c], Jan Kwiatkowski[d], Tomasz Mrugalski[e], Krzysztof Nowicki[e], Wiktor Procyk[b], Konrad Sienkiewicz[a], Robert Szuman[b], Jarosław Śliwiński[c], Jacek Światowiak[e], Piotr Wiśniewski[c], Józef Woźniak[e]

[a] *National Institute of Telecommunications, Warsaw, Poland*
[b] *Poznań Supercomputing and Networking Center, Poznań, Poland*
[c] *Institute of Telecommunications, Warsaw University of Technology, Warsaw, Poland*
[d] *Institute of Informatics, Wrocław University of Technology, Wrocław, Poland*
[e] *Faculty of Electronics, Telecommunications and Informatics, Gdańsk Univeristy of Technology, Gdańsk, Poland*

Abstract—Replacing the IPv4 protocol with IPv6 on the Internet is currently one of the aims of the European Union policy. The main reason for this replacement is the effeteness of the addresses pool in the IPv4 protocol, which can cause serious complications in the evolution of the Internet and its adaptation in new areas, e.g., in next generation mobile telephony or the so called Internet of Things. Simultaneously, the addressing capabilities of the IPv6 protocol are practically unlimited and its new functionalities increase the attractiveness of its usage. The article discusses the problems connected with the IPv6 deployment on the Internet. Especially, the rules for realization of the IPv6 deployment and rules for cooperation of IPv4 with IPv6 (including cooperation tests) in network infrastructure and in applications are presented. Moreover, the European projects' results and the activity's directions of the national project Future Internet Engineering are discussed.

Keywords—Internet evolution, IPv6, migration, mobility, Next Generation Internet, research.

1. Introduction

Work on the new protocol intended to replace IP version 4 (IPv4) began in the early Nineties and led to the adoption by standardization institution Internet Engineering Task Force (IETF) the first standard (RFC 2460) in 1998 for a protocol called IPv6 [1]. One of the main reasons for taking this work was limited address space in IPv4, and very large dynamic allocation of free addresses. In addition, before developing a new IP protocol many new functions were defined, including support for the security, routing, and mobility. Current forecasts for the depletion of free IPv4 addresses made by the Internet assigned numbers authority (IANA) indicate that these addresses will run out between 2010 and 2013. Figure 1 shows the forecast exhaustion of IPv4, depending on the method of determining the rate of increase in the allocation of IPv4 addresses [2]. The paper presents four methods of estimating the growth rate of allocation of free addresses: smooth, polynomial, exponential and linear. In the case of the smooth method, the IPv4 addresses pool is expected to be exhausted before 2011, and in the case of the linear method the addresses pool will be exhausted before 2013. Methods: polynomial and exponential estimate the depletion of addresses during the year 2012. Regardless of the method of research, the prospect of exhaustion of IPv4 addresses is so close that the urgent implementation of IPv6 has become a necessity.

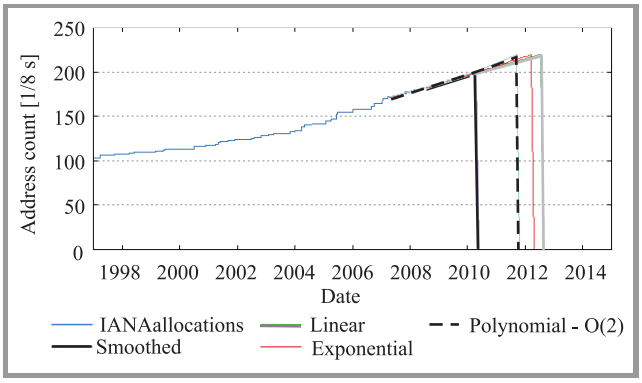


Fig. 1. Forecast rate of IPv4 addresses allocation in the IANA organization.

Use of IP in new application areas, such as mobile phones [3] or the Internet of Things [4] has forced increased budget and efforts on development of the IPv6 protocol and services applications associated with it. At the same time, works on the acceleration of migration processes and the implementation of IPv6 in telecommunication operators networks and end-user operating systems were intensified. The article presents the main features of IPv6 and the development of the protocol in the context of ongoing research projects. Then the state of implementation of IPv6 within research networks environment in Poland is reviewed and the scope of the IPv6 research in the Future Internet Engineering project is covered.

2. IPv6 Functionality

The modern Internet is based almost entirely on the use of the IPv4 protocol developed in the 1970s. At that time no one foresaw the development of the Internet on the scale

observed today, especially the limitations of the available address space size. The problem of availability of addresses space was identified in the Nineties and it was the main reason to work on IPv6. Early estimates concerning the availability of addresses were predicting a few-year period. It is true that since then it has been several years and today it is still possible to obtain IPv4 addresses, although conditions to do it are tightened and much more restrictive than ever before. The demand for IPv4 addresses managed to slow down not only exacerbating the criteria for granting them, but also through the introduction of classless routing (called classless inter-domain routing), a mask of variable length (called variable length subnet mask), dissemination NAT (network address translation) mechanisms, as well as by the ability to configure multiple virtual Web servers on a single public IP address.

Although initial estimates indicated the exhaustion of the address space within just a few years during work on the new protocol assumed a large freedom of design and abolishment of ensuring full backward compatibility with IPv4. Thus, IPv6 is distinguished not only a much larger address space, but offers many other interesting features in regard to confidentiality, authentication, fragmentation only at the sender's side, no checksum in IPv6 datagram and easier to use mobility.

An IPv4 address is 32 bits, giving 2^{32} (approximately 4 billion) possible values, while an IPv6 address has a length of 128 bits giving a staggering number of addresses – more than 340 undecillion (or $6.5 \cdot 10^{23}$ addresses per square meter surface). It is much easier to imagine the enormity of the space by stating that if any device with the Internet connectivity were replaced by a network as big as today's Internet, 64-bit address space would be enough. In the IPv4 protocol support for IPSec (IPSec enables the encryption/authentication of transferred data) is optional, while in the IPv6 protocol it is mandatory. It allows not only to ensure confidentiality but also provides the basis for further extension of the protocol features such as mobility.

IPv6 solves the performance problems observed when using IPv4. In the IPv4 packet might be re-fragmented/defragmented on each node that participates in the exchange of traffic between the sender and the recipient. In IPv6 fragmentation is possible only at the sender side: datagrams have to be in a size not exceeding the smallest MTU of any of the links on the route.

Other changes include fixed length 40 bytes in size of header, removed the header checksum and abandoned a validation of data at each stage of the transmission – all these changes were dictated by the need to reduce the demand for computing power in network devices and shorten the time required for a handling/routing datagram. Nowadays, thanks to technological advances and protocols such as MPLS these features have no longer a significant impact on increasing performance, as in the years when IPv6 was designed.

Today we can observe growing popularity of portable devices with wireless access to the Internet, and support for the mobility is becoming more and more important. Mobility is also possible to be implemented in IPv4 networks, but its use causes many problems. Mandatory implementation of IPSec in IPv6 as well as the large address space make the implementation of mobility in next generation networks using IPv6 much simpler. In addition, the MIPv6 protocol allows mobile terminal moving between networks without changing IP address. The movement of the mobile terminal is transparent to the transport protocol, and upper layer protocols.

During the design process of the IPv6 protocol special emphasis was put on the mechanisms of automatic configuration. There are two possible modes of autoconfiguration. The first one called a stateless configuration allows to configure the basic parameters of the hosts, such as an IPv6 address and routing configuration. The second available mechanism is stateful configuration, implemented using DHCPv6 [5]. Compared to its predecessor known from IPv4, DHCPv6 servers offer redundancy, the possibility of a smooth renumbering/readdressing of the network and configuration of large numbers of additional parameters, such as the delegation of address pools (prefix) instead of individual addresses. Currently 57 configuration options are approved [6] and the IETF is intensively working on further development of mechanisms for automatic configuration.

These features confirm that the IPv6 protocol has been considerably improved in comparison to IPv4. However, there are also some drawbacks. The mentioned lack of backward compatibility affects the pace of implementation of the new protocol and its popularity. Although most modern devices and applications could support both protocols or only the IPv6 protocol, the availability of IPv4 addresses inhibits the implementation of new mechanisms for IPv6. Currently, only the efforts of large corporations operating on the Internet can help to accelerate the migration to IPv6 networks. A good example is Google, which recently applied for the transmission of IPv6 traffic inside Youtube [7], thus increasing the overall level of IPv6 traffic on the Internet by thirty. Other companies are constantly working on developing their applications to adapt them to work with IPv6. For example, the producer of the popular MySQL database system speeds up work on completing the implementation of all modules in order to support IPv6. Last year, communications based on IPv6 protocol between the user of the MySQL system (mysqld) and MySQL server (ndb_mgmd) were implemented, but the communication between the MySQL server (ndb_mgmd) and databases repositories (ndb_d) is still to be implemented, and has been so far performed basing on IPv4 [8].

3. Development of IPv6

For many years IPv6 has been strongly supported as the next generation Internet protocol by both the European Commission and other government organizations, and its

further development and popularization are the target of many projects funded by the European Union and other organizations supporting researches. This section presents a brief overview of the major projects supporting the development of IPv6 in the world. Among the major projects financed by the European Commission are the following projects: 6NET and its continuation 6DISS and 6DEPLOY and Euro6IX. Other presented projects include worldwide Moonv6, Indo-European project 6CHOICE and a Japanese project known as KAME.

The largest research project (at the time of its inception) funded by the European IST program (IST-2001-32161) was a project called Euro6IX [9], which involved leading telecommunication operators operating in Europe. The main objective of the project was to support the rapid deployment of IPv6 in Europe, including works such as designing and implementing a native IPv6 network, the study of advanced network services, application development and active participation in the standardization organizations.

An example of another large European project to stimulate the development of IPv6 is 6NET [10], whose main beneficiaries are the national research & education networks and academic community. The project built a native IPv6 network connecting 16 countries in order to gain experience of IPv6 deployment and migration from existing IPv4 networks. This environment was also used for extended tests of new IPv6 services and applications, as well as interoperability testing with existing applications. Main objectives of the 6NET project were:

- Install and maintain an international pilot IPv6 network including static and mobile components to better understand the problems associated with the implementation of IPv6.
- Test migration strategy for the integration of IPv6 with the existing IPv4 infrastructure.
- Implement and test new IPv6 services and applications as well as existing services and applications on the IPv6 infrastructure.
- Evaluate the address allocation, routing and DNS for IPv6 networks.
- Cooperate with other activities and IPv6 standardization organizations.
- Promote IPv6 technology.

The 6NET project was completed on June 30, 2005, but the popularization, training and support for the IPv6 activity was continued in the 6DISS project [11]. The aim of this project was to promote a broader knowledge of IPv6 through a program of training and knowledge transfer to developing regions. The 6DISS project ended in September 2007, but the training materials and distance learning packages are still available on the Internet free of charge.

The development of the IPv6 protocol is supported by the European Commission also under the Seventh Framework Programme. An example of such two-and-a-half-year project providing training support to IPv6 and its implementation for network operators, service providers and industry, is a project called 6DEPLOY [12]. This project offers not only direct the training of engineers and network administrators but also transfers knowledge and best practices in the topic to other instructors who may benefit from the project materials to teach others. The project has IPv6 training laboratories available remotely to carry out practical exercises, both during seminars and in another time. Also, a professional e-learning course is available through the project site, 6DEPLOY. It uses training materials developed during the IPv6 6DISS (described above) as well as experiences with IPv6 implementation of projects such as 6NET, Euro6IX and GEANT, and the cooperation and contacts established with the IPv6 forum, European IPv6 Task Force and IETF. The project includes thirteen 6DEPLOY partners from the commercial sector and academic research.

An example of another project in the field of IPv6 is a worldwide project Moonv6 [13] established by the IPv6 forum organization. This project focuses on providing technical information related to the implementation of IPv6 and leads the global IPv6 Ready Logo Program [14]. The IPv6 Ready Logo Program is a program of testing and broader cooperation. The steering committee of the IPv6 Ready Logo Program is made up of equipment and service providers, academic institutions, organizations and members of the IPv6 TAHI project (Japan) [15], the University of New Hampshire (USA) IRISA/INRIA (France), European Telecommunications Standardization Institute ETSI, TTA Telecommunications Technology Association (Korea), Beijing Internet Institute BII (China), Chunghwa Telecom Labs CHT-TL (Taiwan) and Japan Approvals Institute for Telecommunications Equipment JATE (Japan). The program of tests for IPv6 Ready Logo is divided into 3 phases:

- **Phase 1** (Silver) logo means that the product includes IPv6 mandatory protocols and can communicate with other IPv6 implementations.
- **Phase 2** (Gold) logo means that the product also meets the strong demands raised by the IPv6 Logo Committee (v6LC).
- **Phase 3** the logo yet undefined during the planning phase, will mean compliance with the same requirements as Phase 2 with the difference that the extended test for the category of IPsec is mandatory here.

Database of the IPv6 Ready Logo Program includes the names of companies that have qualified to use the logo and product names whose samples have been tested and evaluated. Such a logo on the product may be helpful to customers when choosing equipment to work with IPv6 networks.

Another project related to the testing of IPv6 is the Go4IT project [16]. This project is aimed at providing “free” and

universal tools to test IPv6 compliance and cooperation. The aim of this project was implementing software for the testing environment to perform a set of tests developed by ETSI and defined in the notation TTCN-3 (Testing and Test Control Notation Version 3).

Another interesting international initiative co-financed under the Seventh Framework Programme for cooperation in India and Europe to promote IPv6 project is 6CHOICE [17]. Selected were a few priority sectors such as research e-infrastructure and Internet security, mobile wireless networks the next generation, the migration of IPv4 to IPv6 in this project. This project supports close cooperation between scientific networks ERNET and GEANT, as well as between the Indian project GRID (GARUDA) and its European equivalent EGEE. This cooperation has been supporting through a combination of networks and joint planning of services with strong support for IPv6. India is one of the first countries with the possibility of using policy regulations to implement this new protocol on a national scale.

Finally, an example of a national project conducted in the years 1998–2006 in Japan is presented. This project called KAME [18] arose from a combination of the efforts of six companies in Japan in order to provide a free stack of IPv6, IPsec and Mobile IPv6 for different BSD system variants. Products of this project are available on the following operating systems: FreeBSD, OpenBSD, NetBSD and BSD/OS. The project officially ended in March 2006, and almost all implemented in the course of its code was switched to FreeBSD and NetBSD.

As is apparent from the above projects, topics of the next generation networks and in particular IPv6 are strongly supported not only in the European Union, but throughout the world by various governmental organizations, science and industry. It is particularly important for interaction of different proposals in this field and to achieve synergies in the final and successful implementation and popularization of IPv6 in the world and a smooth migration to IPv6 with the existing solutions.

The military projects are also worth mentioning. The U.S. Department of Defense, together with research organizations and the DARPA (Defense Advanced Research Projects Agency) and the DISA (Defense Information Systems Agency) adopted a strategy of migration to IPv6 in October 2001. Since 2010, IPv6 has replaced IPv4, and is referred to as the Mandatory Standard E2E (End-to-End) Protocol. This is a very tangible role in government procurement to be carried out, since only products that have IPv6 support can be offered in tender procedures.

4. IPv6 Implementations in R&D Environment in Poland

The R&D environments were the first interested in testing and development of IPv6 protocol. It was a year after elaboration of IPv6 protocol specification, when network community began to activate IPv6 in test networks and in this way in 1996 the test network 6BONE was built. Also in Poland a few 6BONE servers came into being (mainly in academic centers) offering the tunneled connections IPv6 in IPv4 to all interested units. The 6BONE network was the first environment with the global scope making it possible to become acquainted with the IPv6 protocol, to perform tests and develop services and applications.

A few years before the end of the 6BONE network (the 6BONE network was ended in 2006 year) the MAN networks operators in Poland began to obtain the production IPv6 addresses blocs and afterwards to run IPv6 in their networks. In the year 2003, with mediation of the European network GEANT, the Polish optical network PIONIER was connected to the global IPv6 network. Since this time the IPv6 protocol has been working parallel to the IPv4 in the core of the PIONIER network and is accessible to all metropolitan area networks. The IPv6 traffic is running on two Juniper T320 core routers in Poznań and on one M120 router in Łódź. There are the following routing protocols used: MBGP interdomain routing (for connections to other operators) and IS-IS intradomain routing (between the PIONIER network routers). The PIONIER network provides with the transport network for 22 academic MANs, assuring of access to global IPv6 resources. There are direct peering points with other Polish (e.g., ATMAN) as well as with foreign operators (neighbors research national networks NREN – e.g., academic network SANET in Slovakia). Figure 2 presents MANs with their own IPv6 address blocs.

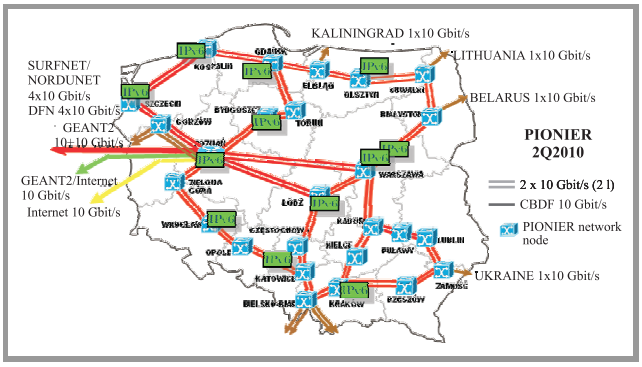


Fig. 2. The PIONIER network map with specified MANs operate IPv6.

The usage of the IPv6 protocol is dependent on resources and services which are accessible using this protocol. In the first row these are such services as ftp, news, servers for WWW, DNS and email. It is also worth mentioning that DNS for national domain .pl has been operating IPv6 since June 2005.

Besides, among the members of the PIONIER network in Poznań and in Warsaw, two nodes of SixXS network POP (point of presence) were activated. These nodes make it possible to connect to the global IPv6 network through tunneling in IPv4. This mode is offered as a transient way for all users, which cannot get the production IPv6 connectivity from their ISP. The node in Poznań activated in January 2005 offers tunnels to the following entities:

Łódź University of Technology, ZETO-Wrocław, Computer Science Institute of Warsaw University of Technology, Polish-Japanese Institute of Information Technology in Warsaw, University of Technology and Life Sciences in Bydgoszcz, Physics Institute of Warsaw University of Technology and AGH University of Science and Technology in Kraków. The SixXS project provides such mechanisms as IPv6 tunnel broker, ghost route hunter and IPv6 monitoring tools [19].

In the year 2004, the Polish IPv6 Task Force was brought into existence and inspired by Poznań Supercomputing and Networking Center [20]. Similar national initiatives (IPv6 Task Forces) exist in many other countries in Europe and in the world. This group is a non-profit initiative concentrating commercial firms, telecommunication operators, services providers, research and education centers – including the PIONIER network members, industrial centers, press and end users. The activity of members focuses on problems like development of network infrastructure, management of networks and security, implementation, development and testing of services and applications, education, experiences exchange, dissemination of results. The IPv6 Polish Task Force has an official web site [20], a publicly available mailing list and public knowledge base WIKI IPv6. The Task Force has cooperated with the Office of Electronic Communications (UKE) – in February 2009, the presentation to promote and stimulate implementation of IPv6 in Poland was worked out together with UKE, and on 24 March 2009 a common, public (PL IPv6-TF + UKE) debate took place to the point of acceleration of the IPv6 implementation in Poland.

In many universities in Poland the IPv6 protocol issues are discussed. For example, since 2002 the ETI department of Gdańsk University of Technology has been permanently running studies (lectures and laboratories) discussing the functionality and usage of the IPv6 protocol in network operation systems and LAN/MAN or WAN networks. Elaborated was also the first publication [21] which discusses the building and configuration of environments using the IPv6 protocol in both native and tunnel modes.

5. The Researched Problems of IPv6 Implementation in Project "Future Internet Engineering"

The importance of the IPv6 subject was noticed by the Ministry of Science and Higher Education and as a result the project Future Internet Engineering (IIP) in which one of the tasks are the research and implementation works in IPv6 technology scope [22] was accepted for realization. In the IIP project the research works related to the IPv6 technology were directed to 3 tasks:

- IPv6 resources virtualization,
- formulation of the cooperation rules and defining of the IPv4-IPv6 tests specification,
- elaboration of IPv6 applications and services.

In the scope of IPv6 resources virtualization the architecture of the "Virtual Internet" system will be designed and developed to make it possible to run users applications and services on dedicated virtual resources in the "on demand" mode.

The crucial element of ongoing works is the formulation of cooperation rules for IPv4-IPv6 protocols and the rules for secure and effective migration of the existing systems to the IPv6 environment. Within the framework of research different scenarios for cooperation of IPv4-IPv6 networks will be formulated and the solutions based on the use of tunneling mechanisms and protocol translation will be proposed. The next step will be the elaboration of good practices related to migration issues and automation of this process together with the tests confirming the correctness of realized activities. The application "IPv6 migration guide" with the knowledgebase (within the scope of IPv6 implementation in popular environments and IT systems or devices) which should support a user (administrator) in this process will come into being. The example dialog window of this application was presented in Fig. 3.

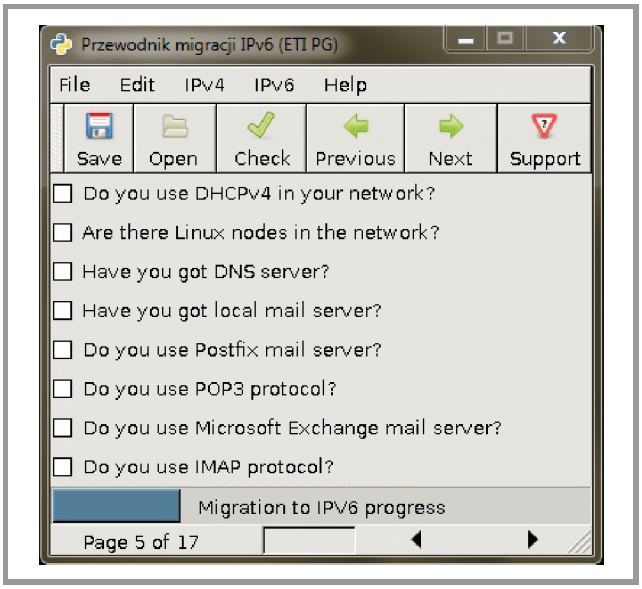


Fig. 3. The example dialog window of „IPv6 migration guide".

Also a version of the "IPv6 migration guide" in the LiveCD form integrated with a software which makes it possible to diagnose the network will be worked out.

The success of the Internet migration to the IPv6 protocol depends on possibilities to conduct this process in a way which does not break the continuity of services availability. Consequently, one of the key phases of this process is the testing of IPv6, which all the market participants should be interested in [23]. One of the first tasks in the scope of IPv6 tests realized in the project is the working out of the conception of tests realization in the small operators networks and the tools to perform these tests. Such choice comes out of the fact that the big entities which have appropriate big budgets and their own development departments can independently prepare and then to carry out the migration

to IPv6. However, in many small firms there is a lack of appropriate know-how in the scope of IPv6 tests and in our opinion they need such support. Within the framework of this task works on the preparation of dedicated tool elaborated based on the TAHI project are currently being performed together with the set of tests adjusted to the small operator needs. We assume that the solution proposed in the project should be characterized by simplicity and availability. From this it follows that the test platform will be realized as dedicated LiveCD distribution of the FreeBSD system with installed TAHI environment. The advantage of such solution is no need to install the FreeBSD system and TAHI environment, which significantly accelerates and simplifies the phase of tests preparation. The tests available within the framework of this solution will make it possible to check the functionalities verified in the scope of cooperation tests. Importantly, they will be performed in a simple configuration which does not require from the one realizing the tests to configure many devices.

The factor which delays the implementation of IPv6 is the configuration complexity comparing to the IPv4 protocol and the lack of dedicated applications and services offering the additional quality. In the project the applications and services working in IPv6 environment will be developed using unique features of this protocol. Elaborated will be a prototype of a VoIP telephone for IPv6 with support of the SIP protocol or an IPTV system basing on the IPv6 network.

As the key element of IPv6 implementation the applications migration should be treated. It is necessary that this migration is running efficiently and does not cause temporary services unavailability. In order to do this it is necessary to work out the cooperation rules in the transient phase, in which the two IPv4 and IPv6 networks will coexist. Considering this, within the framework of the IIP project works will be taken up for the solution to assure the cooperation of IPTV systems based on IPv4 and IPv6 protocols. It will contribute to utilize the currently exploited devices supporting only the IPv4 protocol (e.g., set top box). We assume that the main element of this solution

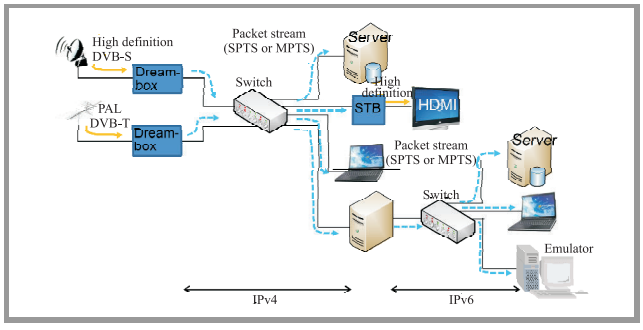


Fig. 4. The IPTV system in IPv4/IPv6 environment. PAL (phase alternating line), DVB-S (digital video broadcasting-satellite), DVB-T (digital video broadcasting-terrestrial), HDMI (high definition multimedia interface), STB (set top box), SPRS (single program transport stream), MPTS (multiple program transport stream).

will be the server placed between IPv4 and IPv6 networks. The main tasks of this server will include the assurance of multicast traffic passing from? the IPv4 to IPv6 network. In this point we should notice that the simple translation mechanisms can be insufficient for this solution because the multicast addresses cannot be translated in a simple way. The important element of the research will be to determine the constraints related to the performance of elaborated solution. However, there is the danger that in case of concurrent servicing of many streams the IPv4/IPv6 translation server can be congested because of its hardware limitations. The proposed solution is presented in Fig. 4.

Additionally, universal programing interfaces (API) between the virtualization system and users applications will be worked out.

What should be mentioned here is the development of comprehensive software served for automatic IPv6 network configuration. The solution called Dibbler is the implementation of DHCPv6 protocol offering the server, client, relay and requestor functionality. Thanks to broad support of various operating systems (Windows 2000-Windows 7, Linux, Mac OS), as well as hardware platforms (x86, amd64, HPPA, Sparc, PowerPC, arm9 etc.), but also because of open source distribution this solution has crowds of users not only in European Union but also in the world. The map of approved users (from over 30 countries) is presented in Fig. 5. Within the framework of the IIP project the significant expansion of functionality with remarkable consideration of the next generation network realities and requirements is anticipated, e.g., the development of servers infrastructure management, better support for mobile nodes.

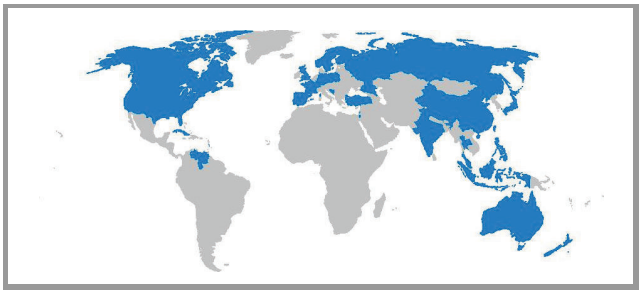


Fig. 5. The map presenting approved users of developed software DHCPv6.

Within the framework of research conducted in Gdańsk University of Technology on the subject of automatic configuration there are also anticipated activities which will aim at standardization of elaborated solutions. The example of such ongoing works is the initiative of standardization of the automatic DS-Lite tunnel configuration mechanism, proposed and accepted by the working group Softwire IETF [24].

In order to simplify the IPv6 solutions configuration in the project the works started to implement the new tunneling method 6RD – Rapid Deployment, defined by IETF in RFC 5569 [25] in January 2010. This method automates

the client access devices configuration for IPv6 protocol including the mechanism for encapsulation of IPv6 datagrams in IPv4. Thanks to this it could be broadly used in building new generation access networks, not only used xDSL, HCF type of access but also WI-FI, WIMAX, etc.

6. Conclusions

This article has presented the arguments for quick implementation of the IPv6 protocol in operators networks, and considered the advantages of this technology comparing to the IPv4 protocol. This technology has the wide support in the scope of its development and implementation in the European Union policy as well as in national initiatives. The best known research projects realized within the framework of European projects and the projects with global meaning were discussed. The status of IPv6 technology implementation in Polish optical network PIONIER and academic metropolitan networks was presented. The important point in the development of IPv6 in Poland are activities performed within the framework of the project Future Internet Engineering.

References

[1] S. Deering, R.Hinden, "Internet Protocol, version 6 (IPv6) Specification", IETF, RFC2460, http://datatracker.ietf.org/doc/rfc2460/

[2] The tool for forecasting of IPv4 allocation addresses speed in IANA, http://www.potaroo.net/tools/ipv4/fig18.png

[3] F. Watanabe, "A view of cellular network migration toward IPv6" [Online]. Available: http://www.apricot.net/apricot2005/slides/C3-3_1.pdf

[4] P. Grossetete, "Internet of Things – The Case of Environmental (IPv6) Monitoring Applications" [Online]. Available: http://ec.europa.eu/information_society/policy/ipv6/docs/ipv6_meeting_march_2009/patrick_grossetete_en.pdf

[5] R. Droms, "Dynamic Host Configuration Protocol for IPv6", IETF, RFC 3315, July 2003.

[6] Dibbler project, http://klub.com.pl/dhcpv6/

[7] C. D. Marsan, "YouTube turns on IPv6 support, net traffic spikes", *PCWorld Mag.*, Feb. 2010.

[8] MySQL 5.1: Reference Manual (January 2009). Section 17.7.2.22.

[9] Euro6Ix project, http://www.euro6ix.net/

[10] 6NET project, http://www.6net.org/

[11] 6DISS project, http://www.6diss.org/

[12] 6DEPLOY project, http://www.6deploy.eu/

[13] Moonv6 project, http://www.moonv6.com/

[14] IPv6 forum, IPv6 Ready Logo Program, http://www.ipv6ready.org

[15] TAHI project, http://www.tahi.org

[16] Go4IT project, http://www.go4-it.eu

[17] 6CHOICE project, http://www.6choice.eu/

[18] KAME project, http://www.kame.net/

[19] SixXS project, http://www.sixxs.net/

[20] Polish Task Force IPv6, http://www.pl.ipv6tf.org

[21] K. Nowicki and J. Światowiak, *Protokoły IPv6. Opis protokołów, materiały do laboratorium*. Wydawnictwo PG, Gdańsk 2001.

[22] W. Burakowski, "Internet Przyszłości – nowa generacja sieci telekomunikacyjnych", *Telekomunikacja i Techniki Informacyjne*, 3-4/2009, pp. 117–126 (in Polish).

[23] J. Ruiz, A. Vallejo, and J. Abella, "IPv6 conformance and interoperability testing" in *Proc. 10th IEEE Symp. Comput. Commun. ISCC 2005*, La Manga del Mar Menor, Spain, 2005.

[24] D. Hankins and T. Mrugalski, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Options for Dual-Stack LiteDS.-Lit", draft-ietf-softwire-ds-lite-tunnel-option-02, March 2010 [Online]. Available: http://tools.ietf.org/id/draft-ietf-softwire-ds-lite-tunnel-option-04.html

[25] R. Despres, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)", IETF, RFC 5569, January 2010.

Jordi Mongay Batalla was born in Barcelona, Spain, in 1975. He received the M.Sc. degree in Telecommunications from Valencia University of Technology in 2000 and Ph.D. from Warsaw University of Technology in 2010. His work experience includes jobs in Centro Nazionale di Astrofisica in Bologna, Italy as well as Telcordia Poland. Currently, he is with National Institute of Telecommunications as Associate Professor. His research interest focus mainly on quality of service in diffserv networks and next generation network architecture. Moreover, he is an active researcher in the challenges related with Future Internet.
e-mail: jordim@tele.pw.edu.pl
National Institute of Telecommunications
Szachowa st 1
04-894 Warsaw, Poland

Artur Binczewski received the M.Sc. degree in Computer Science from the Poznan University of Technology in 1993. He is the Manager of Network Department at the PSNC. He leads the team responsible for development and maintenance of Polish optical network – PIONIER and Poznań metropolitan area network – POZMAN. Artur Binczewski was involved in several EC projects: SEQUIN, ATRIUM, 6NET, EMANICS, FEDERICA, GN1 or GN2. He also coordinated the PORTA OPTICA STUDY, PHOSPHORUS projects and currently the NEWMAN project. His main research activities concerns the architectural aspects of control and management planes in optical networks, protocols for next generation networks and advanced multimedia streaming (4K and beyond digital cinemas).
e-mail: Artur@man.poznan.pl
Poznań Supercomputing and Networking Center
Noskowskiego st 12/14
61-704 Poznań, Poland

Wojciech Burakowski was born in Warsaw in 1951. He received M.Sc., Ph.D. and D.Sc. degrees in Telecommunications from Warsaw University of Technology in 1975, 1982 and 1992, respectively. In 90-ties he was working one year for Telefonica I+D in Madrid as senior engineer. From 1997 he is a professor at Warsaw University of Technology. From 2003 he is Tenured Professor. From 2002 he is Director for Research of Institute of Telecommunications, Warsaw University of Technology. He is a leader of the Telecommunication Network Technologies (TNT) Group. From 1990 he is involved as the member of the Management Committees in the European projects COST 224, 242, 257, and 279, all related to the traffic control issues in the broadband multi-service networks. The TNT group head by Wojciech Burakowski has been involved in targeted EU projects as the Copernicus 1463 (1994–1998) and FR5 IST-AQUILA (2000–2003). Currently the TNT group is involved in 6FR IP project EuQoS (2004–2007) and in 6FR coordination action IST project MOME (2004-2006). Professor Wojciech Burakowski is the author or co-author of about 130 papers published in books, international and national journals and conference proceedings. He is a chairman and member of technical program committees of many national (KST, PSRT) and international conferences (NATO RCMCIS, PGTS, ACS, NETWORKING, AINA). He was the leader of many national projects and co-author of more than 60 technical reports. He was the supervisor of 11 Ph.D. thesis. His research areas include ATM, IP, and heterogeneous networks (fixed and wireless), traffic engineering, simulation techniques, measurement methods and test-beds. Awards: in 2003 the TNT Group received Rector's Award for scientific achievements.

e-mail: wojtek@tele.pw.edu.pl
Institute of Telecommunications
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

Krzysztof Chudzik received his M.Sc. in automation and robotics in 1995 and Ph.D. in Computer Science in 2003 from Wrocław University of Technology. Since 2003 he is with Institute of Informatics, Wrocław University of Technology as an assistant and since 2007 as an adjunct. His main scientific interest include: network systems, computer networks and discrete optimization.

e-mail: Krzysztof.Chudzik@pwr.wroc.pl
Institute of Informatics
Wrocław University of Technology
Wybrzeże Wyspiańskiego 27
50-370 Wrocław, Poland

Bartosz Gajda received the M.Sc. degree in Computer Science from the Poznań University of Technology, in 1998. Since 1997 he has been working in Poznań Supercomputing and Networking Center (PSNC) where he is responsible for network management systems. His main interests concern computer networks, network protocols, network management, QoS and IPv6. He is also in charge of development IPv6 network in PSNC and in PIONIER NREN network, and projects involved with IPv6 (6NET, EMANICS, Future Internet Engineering).

e-mail: Gajda@man.poznan.pl
Poznań Supercomputing and Networking Center
Noskowskiego st 12/14
61-704 Poznań, Poland

Mariusz Gajewski has been employed at the National Institute of Telecommunications since 1998. He received his M.Sc. degree in Telecommunications from the Warsaw University of Technology, Poland. He specializes in technical aspects of network architecture, NGN and IP networks, as well as Future Internet.

e-mail: M.Gajewski@itl.waw.pl
Internet Architectures and Applications Department
National Institute of Telecommunications
Szachowa st 1
Warsaw, Poland

Adam Grzech Ph.D., D.Sc. He is a professor in the Institute of Computer Science, Department of Computer Science and Management, Wrocław University of Technology (WUT). He obtained M.Sc. degree from Department of Electronics, Wrocław University of Technology in 1977, Ph.D. degree from Institute of Technical Cybernetics, Wrocław University of Technology in 1979, D.Sc. degree from Department of Electronics, Wrocław University of Technology in 1989 and professor title from

President of the Republic of Poland in 2003. His research interests include design and analysis of computer systems and networks, requirement analysis, modeling and identification of computer networks, design and application of local and wide area computer networks, flow control and congestion avoidance in computer networks, migration and integration of heterogeneous computer systems and networks, services integration in networks, intelligent networks, quality of service – aware networks, SOA-paradigm based systems, engineering of the future internet, security of computer systems and networks, agent-based systems and its application in optimization and control and intelligent information systems. He is an author and co-author of 218 papers published in books, journals and conference proceedings, supervisor of 8 completed Ph.D. thesis and supervisor of more than 200 completed M.Sc. thesis in computer engineering.

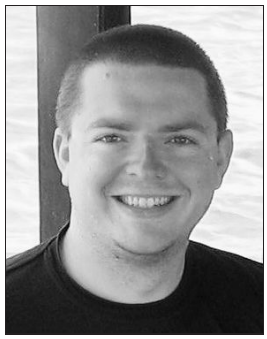
e-mail: Adam.Grzech@pwr.wroc.pl
Institute of Informatics
Wrocław University of Technology
Wybrzeże Wyspiańskiego 27
50-370 Wrocław, Poland

Piotr Krawiec received the M.Sc. degree in Telecommunications from the Warsaw University of Technology, Poland, in 2005. Now he works as assistant at the Institute of Telecommunications, Warsaw University of Technology. He is with Telecommunications Network Technologies (TNT) Group at the Institute of Telecommunications, WUT, from 2005. His research interests focus on quality of service in IP networks, NGN architecture and new networks techniques.

e-mail: pkrawiec@tele.pw.edu.pl
Institute of Telecommunications
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

Jan Kwiatkowski received his M.Sc. and Ph.D. in Computer Science from the Institute of Technical Cybernetics, Wrocław University of Technology, at 1977 and 1980, respectively. Since 1980 he works as an adjunct at the Faculty of Computer Science and Management, Wrocław University of Technology. In the years 1987–1998 he acted as a deputy director responsibly for education in the Faculty of Computer Science and Management, Wrocław University of Technology. In the years 2002–2004 under sabbatical leave, he worked as associate Visiting Professor at Math and Computer Science Department at the University of Missouri, St. Louis. His area of scientific interest includes software engineering and parallel processing. He is mainly interested in parallel and distributed software design process, performance evaluation of parallel programs and cluster/grid computing.

e-mail: Jan.Kwiatkowski@pwr.wroc.pl
Institute of Informatics
Wrocław University of Technology
Wybrzeże Wyspiańskiego 27
50-370 Wrocław, Poland



Tomasz Mrugalski received his M.Sc. (Computer Science) and Ph.D. (Telecommunication) degrees from Faculty of Electronics, Telecommunication and Informatics, Gdańsk University of Technology (GUT) in 2003 and 2010, respectively. He worked for Intel Corp. for 7 years, where he gained practical experience with experimental WiMAX and other high performance hardware. He recently joined Internet Systems Consortium (ISC), a California based non-profit corporation that develops commercial quality open source software and also operates one of 13 DNS root servers. He is actively involved in IETF and is authoring or co-authoring 5 drafts, with one of which was approved recently and expects publication as RFC later this year. His activities are mainly related to DHCPv6, IPv6 in general and open source software development. He is a member of Steering Committee of Polish IPv6 Task Force and leads several open source projects: "Dibbler" (open source, portable DHCPv6 implementation), "Numbat" (IPv6/Mobile WiMAX simulation environment) and "ip46nat" (experimental kernel-space IPv4-to-IPv6 traffic translation). He is also author or co-author of over 15 journal and conference papers.

e-mail: Tomasz.Mrugalski@eti.pg.gda.pl
Faculty of Electronics, Telecommunications
and Informatics
Gdańsk University of Technology
Gabriela Narutowicza st 11/12
80-233 Gdańsk, Poland

Krzysztof Nowicki received his M.Sc. and Ph.D. degrees in Electronics and Telecommunications from the Faculty of Electronics at the Gdańsk University of Technology, Poland, in 1979 and 1988, respectively. He is an author or co-author of more than 100 scientific papers and an author and co-author

of five books. His scientific and research interests include network architecture, analysis of communication systems, network security problems, modeling and performance analysis of cable and wireless communication systems, analysis and design of protocols for high speed LANs.

e-mail: know@eti.pg.gda.pl
Faculty of Electronics, Telecommunications
and Informatics
Gdańsk University of Technology
Gabriela Narutowicza st 11/12
80-233 Gdańsk, Poland

Wiktor Procyk received the M.Sc. degree in Computer Science (Software Engineering) from the Poznań University of Technology in 2000. Since 1997 he has been cooperating with Poznań Supercomputing and Networking Center (PSNC). Now he is working as a Network Specialist in PSNC NOC. His main interests concern network management, traffic analysis and measurement, passive and active measurements, QoS and IPv6. He is also in charge of development IPv6 network in PSNC and in PIONIER NREN network. He actively participates/participated in projects involved with IPv6 (6NET, EMANICS, Future Internet Engineering).

e-mail: wiku@man.poznan.pl
Poznań Supercomputing and Networking Center
Noskowskiego st 12/14
61-704 Poznań, Poland

Konrad Sienkiewicz has been employed at the National Institute of Telecommunications since 1997. He holds a graduate degree in Telecommunications from Warsaw University of Technology, Poland (1997). He specializes in technical aspects of network architecture, NGN and IP networks, as well as Future Internet.

e-mail: K.Sienkiewicz@itl.waw.pl
Internet Architectures and Applications Department
National Institute of Telecommunications
Szachowa st 1
Warsaw, Poland

Robert Szuman graduated from Poznań University of Technology in 2000 and got the M.Sc. degree in Computer Science (Databases and Networks Designing). Since 1999, he has been co-operating with Poznań Supercomputing and Networking Center (PSNC), where he started work in the Network Department as a Network Management Systems Administrator. Now he is working as a Network Specialist in PSNC. His main fields of research interests are network management systems administration and configuration, broadband and optical networks monitoring, quality of service in computer networks, traffic analysis and measurement technologies, network management protocols, tools and procedures used by the Network Operation Center (NOC).

e-mail: rszuman@man.poznan.pl
Poznań Supercomputing and Networking Center
Noskowskiego st 12/14
61-704 Poznań, Poland

Jarosław Śliwiński was born in Toruń, Poland, in 1979. He received M.Sc. and Ph.D. degrees from Warsaw University of Technology in 2003 and 2008, respectively. His research interests cover traffic control, systems' design and implementation methodology.

e-mail: J.Sliwinski@tele.pw.edu.pl
Institute of Telecommunications
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

Jacek Światowiak graduate Faculty of Electronics, Telecommunications and Informatics Gdańsk University of Technology (GUT). Since 2002, lecturer of postgraduate studies at GUT. Co-authored the script for students of computer science: "Protocols of IPv6 – description of the protocols. Laboratory materials" and author of the book "Windows Server 2003/2008. Environmental safety with Forefront Security". The holder of many certificates: MCP, MCSE + M, MCSE + S, 11 MCTS certifications, 7 MCITP, MCT – Microsoft

Certified Trainer and the honorary title of MVP (Microsoft Most Valuable Professional) for forefront technology.
e-mail: Jacek.Swiatowiak@lan-net.pl
Faculty of Electronics, Telecommunications
and Informatics
Gdańsk University of Technology
Gabriela Narutowicza st 11/12
80-233 Gdańsk, Poland

Józef Woźniak is a Full Professor in the Faculty of Electronics, Telecommunications and Computer Science at Gdańsk University of Technology. He received his Ph.D. and D.Sc. degrees in Telecommunications from Gdańsk University of Technology in 1976 and 1991, respectively. He is an author or co-author of more than 250 journal and conference papers. He has also coauthored 4 books on data communications, computer networks and communication protocols. In the past he participated in research and teaching activities at Politecnico di Milano, Vrije Universiteit Brussel and Aalborg University, Denmark. In 2006 he was Visiting Erskine Fellow at the Canterbury University in Christchurch, New Zealand. He has served in technical committees of numerous national and international conferences, chairing or co-chairing several of them. He is a member of IEEE and IFIP, being the vice chair of the WG 6.8 (Wireless Communications Group) IFIP TC6 and. For many years he chaired the IEEE Computer Society Chapter at Gdańsk University of Technology. His current research interests include modeling and performance evaluation of communication systems with the special interest in wireless and mobile networks.

e-mail: jowoz@eti.pg.gda.pl
Faculty of Electronics, Telecommunications
and Informatics
Gdańsk University of Technology
Gabriela Narutowicza st 11/12
80-233 Gdańsk, Poland

Piotr Wiśniewski was born in Warsaw, Poland, in 1985. He received M.Sc. degree in Telecommunications at Warsaw University of Technology in 2010. Since 2010 he has been Ph.D. student.

e-mail: pwisniewski@tele.pw.edu.pl
Institute of Telecommunications
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

Paper

IPv6 in Virtualization Environments

Krzysztof Chudzik and Jan Kwiatkowski

Institute of Informatics, Wrocław University of Technology, Wrocław, Poland

Abstract—The primary network layer protocol on which the operation of most computer networks is based, including the Internet is the Internet protocol version 4 (IPv4). Due to the limitations of this protocol, it is becoming increasingly widespread use of the Internet protocol version 6 (IPv6). The IPv6 implements some new features not available in IPv4. The paper provides a short overview of the key features of IPv6 and discussed the possible levels of network virtualization. The research environment to testing the level of support for IPv6 protocol by virtualization environments is proposed. The results of tests conducted using the proposed research environment for Hyper-V virtualizer are presented.

Keywords—Hyper-V virtual machine, IPv6 protocol, virtualization environment.

1. Introduction

The primary network layer protocol on which the operation of most computer networks is based, including the Internet is the Internet protocol version 4 (IPv4). Due to the limitations of this protocol, it is becoming increasingly widespread use of the Internet protocol version 6 (IPv6) [1], [2], [3]. The IPv6 implements some new features not available in IPv4. The interoperability features with IPv4 is not implement in IPv6, then IPv6 creates essentially a independent (parallel) network to IPv4. The traffic between both networks requires special translators, however most of existing operating systems supports both protocols.

Implementation of IPv6 cannot ignore the virtual environments, which the main tasks are abstraction and isolation of widely understood network resources, including computer networks, network devices, computers, operating systems, applications, services, etc.

In the paper the research environment to testing the level of support for IPv6 protocol by virtualization environments is proposed. The results of tests conducted using the proposed research environment for Hyper-V virtualizer are presented.

The paper is organized as follow. Section 2 provides a short overview of the key features of IPv6. Section 3 describes the coexistence of IPv6 and IPv4. The main topic of Section 4 are the levels of network virtualization. In Section 5 interface for IPv6 application using virtual environment is proposed. In Section 6 the research environment for testing the level of support for IPv6 protocol by virtualization environment is proposed. Section 7 presents results of testing the Hyper-V virtualizer. Finally, Section 8 outlines the work and discusses the further works.

2. Key Features of the IPv6

The first documents relating to IPv6 were published in the 90s: RFC 1883 [4] document was issued in 1995 and shortly afterwards obsoleted by RFC 2460 [5] in 1998. The latter is constantly updated. According to information given at the Internet Engineering Task Force (IETF) website[1] the last update of this document occurred in May 2010 (the state of the art at the time of writing in June 2010). As described in [5], IPv6 is a new version of the Internet protocol, designed as the successor to IPv4 [6]. The most significant changes and improvements introduced by IPv6 are as follows [5]:

Expanded addressing capabilities. The IP address size increases from 32 bits to 128 bits. This is the solution of the most pressing problem, namely the shortage and depletion of the pool of free IPv4 address. The resulting new larger pool of addresses can support a much greater number of networks and nodes. By that means, the new protocol permits to avoid temporary solutions as network address translation (NAT), which causes problems because a number of network devices uses and is represented in the Internet by the same public address and there is no way to distinguish between them from the Internet side. Larger address space allows to create new mechanisms to facilitate the configuration of network devices, such as stateless auto-configuration of addresses with the use of the MAC addresses and the IPv6 prefixes advertised by routers. IPv6 allows more levels of addressing hierarchy, which simplifies scalability and routing, including the routing of multicast traffic which replaces the broadcast traffic in IPv4. Some new types of addresses are defined, such as an anycast addresses.

Header format simplification. Some IPv4 header fields have been dropped or made optional to reduce the cost of packet processing and usage of bandwidth [5]. The IPv6 header has fixed length and is optimized for processing up to 64 bits at a time (32 in IPv4). Routers do not calculate any IPv6 header checksum as do that in IPv4. Routers also are not responsible for fragmentation of oversized packets. They only signal the source to send smaller packets [3].

[1] http://www.ietf.org

Improved support for extensions and options. The RFCs [4], [5] assume that changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

Flow labelling capability. IPv6 allows labelling of packets. Packages may be labelled as belonging to a certain type of network traffic, which requires special handling by quality of services (QoS), for example the traffic associated with VoIP services.

Authentication and privacy capabilities. In the RFCs [4], [5], it was stated that extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6. This statement is sometimes a source of serious misunderstandings, because only support is mandatory, not the use for example IPSec. IPv6, in itself, is not more secure than IPv4, but the process of implementing security mechanisms is easier, because there is no address translation (NAT), and some problem may be omitted. In addition, the vast IPv6 address space is not densely populated by nodes, which makes it difficult to scan a network looking for potential victims of the attack [3].

3. IPv6 and IPv4 Coexistence

Because of significant differences between protocols, the transition from IPv4 to IPv6 can not be done in one step, but must be carried out the migration process. The lack of IPv6 backward compatibility causes the two protocols IPv6 and IPv4 must be used simultaneously, often on the same node. Certain services are available to the node over IPv6, while others over IPv4. This requires a dual stack of IP protocols and in fact is done on nodes that have IPv6 support, for example the operating systems which support both protocols are configured with both types of addressees and are equipped with utility programs that support both protocols. Usually there is configured a kind of priority of IPv6 over IPv4 and IPv4 are used where access to a service or node are not possible by the use of IPv6.

The above resolves the problems of communication in environments where IPv6 is implemented and the routing of IPv6 is supported. In the most cases, in the migration process, communication problems associated with incomplete or no implementation of the IPv6 routing occurs. Since IPv4 and IPv4 routing is usually a fully implemented, the IPv6 network traffic can be tunnelled through existing IPv4 networks. The tunnels use encapsulation of IPv6 in IPv4 packet and usually add the IPv4 header before the IPv6 packet at the point of entry to the tunnel. In this form, the packet is transmitted by the networks that support only IPv4. At the other end of tunnel, the unnecessary IPv4 header is removed and the original packet is transmitted to its IPv6 destination (Fig. 1).

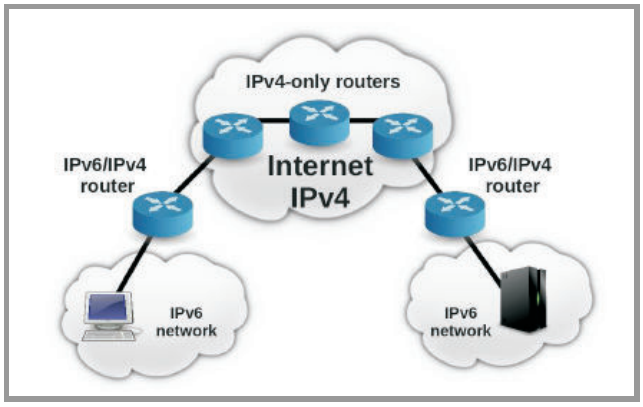


Fig. 1. The IPv6 communication over IPv4 Internet.

One can configure tunnels manually or use automatic configuration. Currently at least five different automation methods are defined [3]:

Transition mechanisms for IPv6 hosts and routers (RFC 2893) [7]. The IPv6 addresses of nodes consist of two parts: the first is a series 96 zero bits (denoted as the prefix ::/96), and the second is the 32-bit IPv4 address, so the transformation between the corresponding IPv4 and IPv6 addresses is trivial. Although not formally deprecated by an IETF standards action, automatic tunnelling should be considered obsolete [3].

6over4: Transmission of IPv6 over IPv4 domains without explicit tunnels (RFC 2529) [8]. 6over4 is used within a single organization or site network. 6over4 treats an IPv4 network as a IPv6 subnet, which delivers basic services for IPv6 hosts, including IPv6 address autoconfiguration and support for multicast. Because of this requirement, the discussed method of tunneling is not often implemented, due the lack of support for multicast traffic in contemporary IPv4 networks [3].

ISATAP: Intra-site automatic tunnel addressing protocol (RFC 5214) [9]. ISATAB, similarly to 6over4, is used within a single organization or site network and that network is treated as non-broadcast multiple access (NBMA). The mechanism is designed for dual-stack nodes to connect them via IPv4-only networks. The IPv6 addresses are constructed in modified EUI-64 format with the use of IPv4 addresses and the universal/local and individual/group bits, which allow take decisions about routing to destination and tunneling [3], [9].

Teredo: Tunneling IPv6 over UDP through NATs (RFC4380) [10]. In RFC 4380 a service is proposed that enables nodes located behind one or more IPv4 network address translations (NATs) to obtain IPv6 connectivity by tunneling packets over UDP. Teredo service requires to operate so-called “Teredo servers” and “Teredo relays”. The teredo servers manage a small fraction of the traffic between teredo clients, while the teredo relays act as IPv6 routers between the teredo service and the “native” IPv6 Internet [11].

6to4: Connection of IPv6 domains via IPv4 clouds (RFC 3056) [11]: This is one of the more popular methods, and is implemented in most modern operating systems [3]. This method provides a link between isolated areas of the operation of IPv6 trough the areas of the operation of IPv4.

Each node with a routable IPv4 address can create a special 48-bit long prefix of IPV6 address to communicate which consist of 2002(hex) followed by IPv4 address in the hexadecimal form. Due to the construction of an IPv6 address mutual conversion between IPv4 and IPv6 is trivial. When node sends a packet, that packet is encapsulated in the IPv4 packet and the destination address is taken from IPv6 address. The communication between IPv6 areas is supported by dedicated relays/gateways [3], [11].

4. Introduction to Virtualization Environments

There are many benefits related to using virtualization, the most important are as follows:

- Reduction of hardware maintenance cost due to using the lower number of physical servers.
- Preventing application from impacting another application when upgrades or changes are made.
- By developing a standard virtual server, it is possible in easy way make its duplication which speed up server deployment.
- Better utilization of available resources.
- Deploying multiple operating system technologies on a single hardware platform.

Additionally virtualization gives opportunity of using the concept of parallel Internets as an innovative way to enable end-to-end service differentiation at the IP level in terms of not only traditional QoS such as delay and loss, but also resilience and availability. Specifically, parallel Internets are coexisting parallel networks composed of interconnected per-domain planes. Network planes are setup to transport traffic flows from services with common connectivity requirements. The traffic delivered within each Network plane has particular treatment in both forwarding and routing [12].
Virtualization, as a mechanism of abstraction and isolation of network resources with support for IPv6, can be implemented at different levels of the network environments; communication and operating system levels respectively.

4.1. Virtualization at the Level of Communication Devices

At the communication device virtualization level, communication and address spaces can be created. The division may occur at layer 2 of ISO/OSI model related to the physical addressing and switching or at layer 3 associated with the logical addressing and routing. Within layer 2, for example, virtual local area networks (VLANs) can be created and IPv6 can be used by the network administrator to have access to switching hardware (Fig. 2).

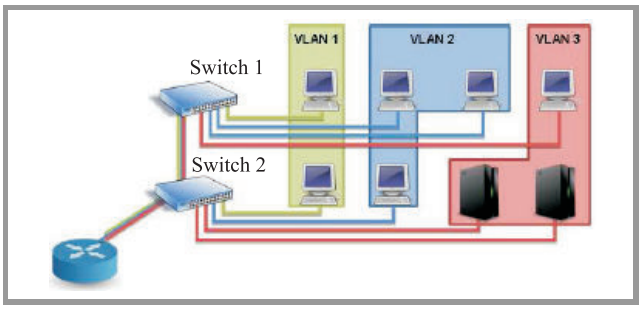


Fig. 2. An example of VLAN virtualization at layer 2.

However, at layer 3, one can create, for example, virtual private networks (VPNs) and IPv6 can be both a transport (tunneling) protocol and transported (tunneled) protocol (Fig. 3).

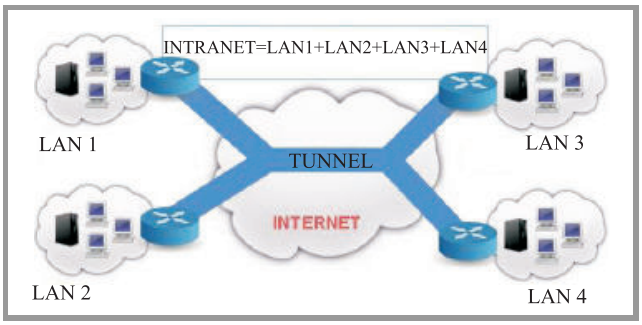


Fig. 3. An example of VPN tunnels virtualization at layer 3.

At the level of communication devices, communication hardware virtualization is possible. For example, multiple routers and/or switches infrastructure, which are interconnected by virtual networks, can be created within a single router or switch. Handling and support for IPv6, using virtualization at the level of communication, are implemented by the functionality of hardware and operating systems (an operating system at this level can operate, for example, as a software firewall and access router to support VPN tunnels).

4.2. Virtualization of Operating Systems, Applications and Services

At the virtualization of operating system level, hardware resources are shared among multiple virtual executive environments. These are the types of virtualization.
Full virtualization. In the base system (host), the total abstraction and emulation of existing or fictitious hardware is carried out. In this abstract emulated environment, an operating system (guest) is executed. Virtualized system operates as if it were running directly on physical hardware.
Paravirtualization. At the base system, hardware abstraction is carried out, but the virtual hardware presented to virtualized system is similar (not necessarily identical) to the real hardware. In addition, paravirtualization will not

work with any operating system, but the operating system has to be adapted to this type of virtualization.

Container virtualization. Container virtualization systems provide the option to run multiple applications in isolated environments, with adequate security on a single operating system. The mechanism of operation is based on the creation of many user spaces that are properly isolated.

Service virtualization. Similar in its operation to the container virtualization. The main difference is that the virtual machine is created when the service is requested and then hardware resources and the environment in which the machine can run are localized.

In the case of virtualization at the level of operating systems, applications and services, handling and support for IPv6 can be implemented by virtualized operating systems, applications and services as well as the virtualization environment itself.

5. Interfaces for IPv6 Applications

At the application level different types of applications with different functional as well as non-functional requirements can be used. Moreover, different system and user interfaces can be used depending on application requirements. It causes the necessity of developing the general, flexible interface that can be used by all available applications. Assuming that the global system is built as a federation of independent execution systems connected by the computer network, it causes that the execution systems should hide their internal complexity by offering a common interface to their internal resources. Additionally, each of the execution systems works in the autonomous manner, ensuring efficient local resources utilization. To fulfil above requirements the system that consist of two cooperating modules: the execution virtualization module and resource allocation module is proposed. The proposed system offers a service abstraction on the highest level with efficient resources utilization performed inside each of execution systems [13].

The execution virtualization module implements an application (service) execution interface, used to hide the underlying hardware-specific details. The virtualization makes it possible to utilize a variety of hardware resources dynamically selected to ensure efficient service execution performed in accordance to the requirements. It aggregates, interprets and utilizes the monitoring data to select the service execution location and execution details. The execution virtualization module virtualizes the necessary resources for the realization of services.

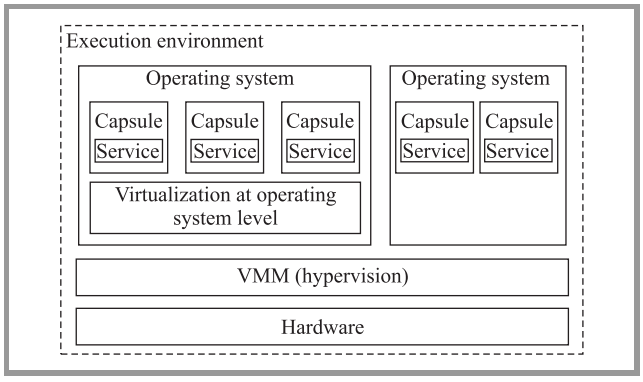


Fig. 4. Two-level virtualization system.

Figure 4 presents two-level virtualization system used by the execution virtualization module. The structure of the system is as follows, over the VMM (hypervisor) level different so called hard virtualizators (full virtualization or paravirtualization) are used. The first level gives opportunity of using different operating system at the same hardware that can provide different services offered by installed application. In the second virtualization level the container virtualizators are used and it enables to have a copy of the same service that can be used by different users. The resource allocation module is responsible for choosing the most suitable execution system for a service request. The execution system running the service is chosen basing on the information about the available computational resources, virtualizers, operating systems and services.

The benefits of using the proposed system are as follows:

- Reduce system response time by accelerating the time of the service execution through an appropriate resources allocation.
- Reduce the number of running services. It reduces the cost of management.
- Hiding the specific implementation. It gives the opportunity to build distributed systems datacentres adjusted dynamically to the requirements.
- The advantages of virtualization are applied, too.

6. Testbed for Testing IPv6 Support by Virtualization Environments

The verification of handling and active support for IPv6 is required due to the large number of virtualization environments, virtualized systems and their different operation. For given a virtualization platform (the host system) and virtualized systems (the guest systems), which create a virtualization environment, a research virtualization environment is proposed and presented in Fig. 5.

The proposed testing environment consists of three virtual networks and one bridging network between the virtual environment and the host system. The environment allows to test routing and routing protocols to determine the impact of host and the opportunity to interact with external devices. It is the minimal configuration, in which there are no contiguous network. This allows to test the routing protocols, both internal and external manner. If in a small network routing protocol is working correctly, it means that its messages are exchanged correctly and has no negative impacts of the host.

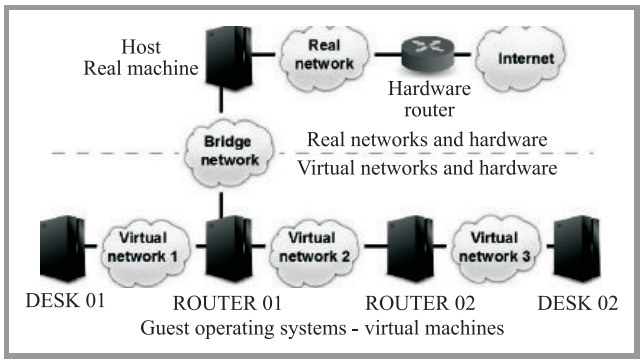


Fig. 5. Example of an IPv6 research environment.

The scope of research conducted with the use of this environment may include:

- Support offered by the virtualization environment to operating systems working on the basis of IPv6. Useful environment should support the main operating systems in the server market, that is, Unix / Linux and MS Windows.
- Creation and configuration of virtual networks with IPv6 as the main protocol at the network layer. Ability of creation networks with different levels of isolation should be taken into account:
  - the networks that are completely isolated. This kind of network should support communication between guest operating systems;
  - the networks for connection between a guest operating system and the host (bridge networks);
  - the networks that are attached directly to the network infrastructure to which the host computer is connected to. This kind of network should provide direct communication between the guest operating systems and real external network environment.
- Support for IPv6 routing and routing protocols, in particular, whether the flow of packets in virtual networks is the same as in real networks, and whether the host system does not interfere with the flow.
- Active support for IPv6 network services, for example, determining whether one is able to start the DHCP server on the side of the host system, which will provide the configuration parameters of the IPv6 network interfaces at the guest systems. Integration of virtual IPv6 networks with real IPv6 networks. The problem involves finding whether there is a possibility of packets routing from internal virtual networks outside the host system and physical access to the host system physical network cards for guest operating system so they can directly use physical networks cards to communication with real networks.
- Support the integration of IPv6 with IPv4 in tunnelling and the direct communications.

7. Testing Hyper-V Virtualizer

The verification of handling and active support for IPv6 in the Hyper-V virtualization environment is required due to the large number of possible applications of this environment. Presented in this section results of the Hyper-V virtualizer testing has been obtained using the research environment presented in the previous section. The proposed by us testing method covers the basic functionality of the Hyper-V environment and simultaneously the MS Windows server 2008R2 operating system (the latest available version), within which we ran Hyper-V as a host operating system. The study used a virtual machines with the same operating system as the guest operating system. The aim of the study is to examine how the Hyper-V environment and the MS Windows server 2008 R2 operating system operate as the host and guest systems using IPv6 as the only communication protocol. The study covered the basic functionalities and services of the IPv6 protocol. Hence the basic idea of the research is related to automatic and static addressing. The examination includes the ability to creating and configuring virtual networks also.

Hyper-V was installed and started in the Microsoft Windows 2008 R2 enterprise edition operation system. The process of installation is easy and limited to installation of a role of Hyper-V with usage of a role installation wizard only. The fully functional virtualization environment is available immediately after the installation. The virtual networks and the virtual machines were created and configured in this environment as shown in Fig. 5. There were no problems with the creation of virtual networks or virtual machines. The host computer and the virtual machines

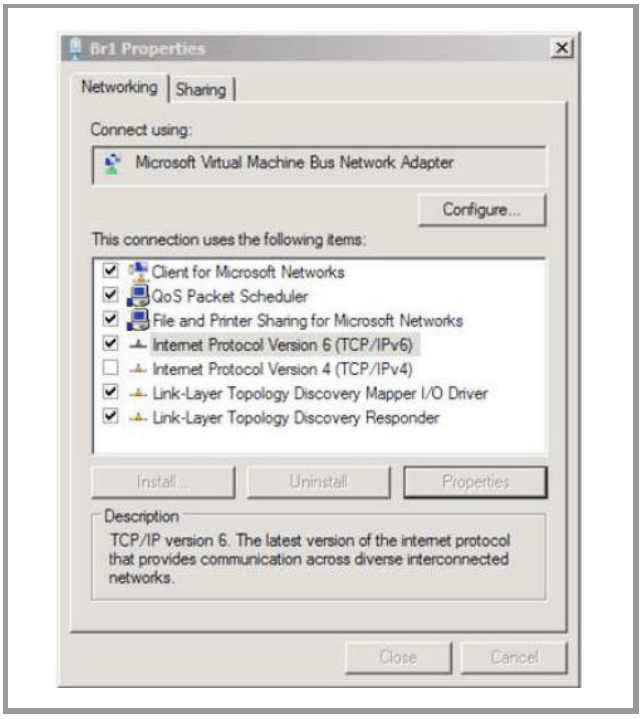


Fig. 6. The static IPv6 configuration.

were configured only with IPv6 addresses to avoid IPv4 issues, as shown in Fig. 6.
Additionally, the firewalls were disabled on the host and the virtual machines to avoid the impact of firewalls on the test results.

7.1. The Link-Local Addressing and Connection Test

The purpose of the test is to check the functioning of the "link-local" addresses in the Hyper-V environment on the host and the virtual machines. These addresses are assigned automatically, so the first step is to inventory the assigned addresses. The inventory results are shown in Fig. 7. Obviously, addresses are unique to this particular environment and test.

Machine	Interface	Adresses
Host (poseidon)	WAN	fe80::c075:cbff:ff0b:223c%11
	Br1	fe80::fde3:5f82:5c69:f54d%17
Server01	Virt1	fe80::99a1:8948:b04f:bc22%13
Router01	Virt1	fe80::380f:e18b:6ecf:b190%14
	Br1	fe80::7dea:4edf:66a0:ebef%11
	Virt2	fe80::f8c1:a7fb:a249:2de%15
Router02	Virt2	fe80::45e1:bd5:ee74:abf9%13
	Virt3	fe80::e8af:5fac:1dae:987%20
Server02	Virt3	fe80::349c:ddea:2a08:b0b9%13

Fig. 7. The local-link addresses assigned to network interfaces during test.

After the inventory, the connection between all the interfaces working in the same virtual networks have been tested using the ping utility. There were no communication issues. Furthermore, it was found that in contrast to Linux, the machines with multiple network cards do not need to enter the identifier of the interface through which communication is to take place. The ping command in Linux is as follows:

- ping6 [-I ⟨device ⟩]⟨link-local-ipv6address⟩,
- ping6 -I eth0 fe80::c075:cbff:ff0b:223c.

The usage of the ping command in Windows remains typical: ping fe80::c075:cbff:ff0b:223c.

7.2. The Static Addressing Test

The purpose of the test is to check the functioning of the manually configured addresses in the Hyper-V environment on the host and the virtual machines. The addresses are configured manually in the dialog windows presented in Fig. 8 according to the address schema presented in Fig. 9.
After the configuration of addresses the tests of connectivity between all the interfaces working in the same virtual networks have been carried out using the ping utility. There were no communication issues.

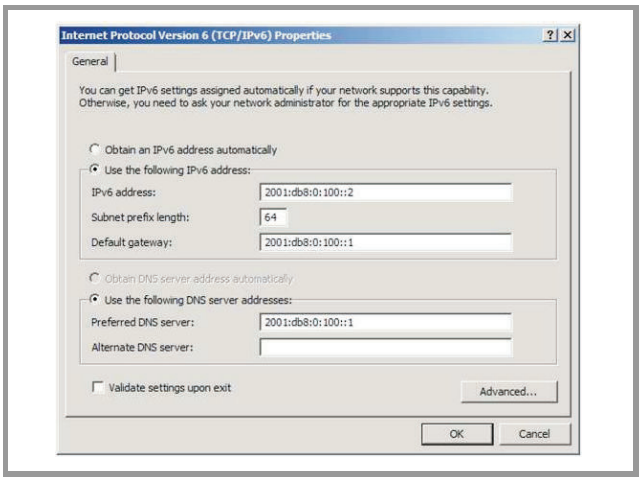


Fig. 8. IPv6 address configuration dialog window.

Machine	Interface	Adresses (Gateway (if present))
Host (poseidon)	WAN	none
	Br1	2001:db8:0:100::1
Server01	Virt1	2001:db8:0:1::2 (2001:db8:0:1::1)
Router01	Virt1	2001:db8:0:1::1
	Br1	2001:db8:0:100::2 (2001:db8:0:100::1)
	Virt2	2001:db8:0:2::1
Router02	Virt2	2001:db8:0:2::2 (2001:db8:0:2::2)
	Virt3	2001:db8:0:3::1
Server02	Virt3	2001:db8:0:3::2 (2001:db8:0:3::1)

Fig. 9. The static IPv6 address.

7.3. The Static Routing Test

The purpose of the test is to check the functioning of static routing in the Hyper-V environment. The network interface addresses were configured according to Fig. 9 and routers were configured as shown in Fig. 10.

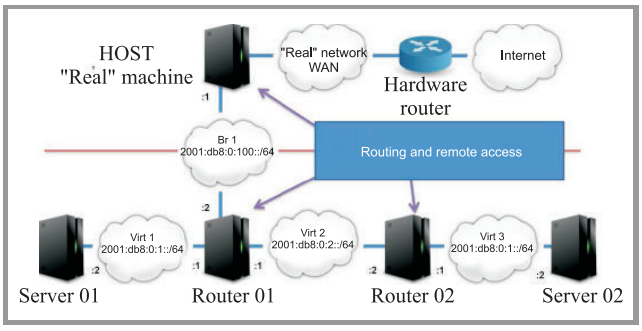


Fig. 10. The router placement in the test environment.

The connectivity test were run between the host computer and the virtual machine and between the virtual machines as shown in Fig. 11. The conclusion is that the static routing works correctly and there are no connection issues. Since the routing protocols are not implemented in MS Windows server 2008 R2, the tests of routing protocols have not been carried out.

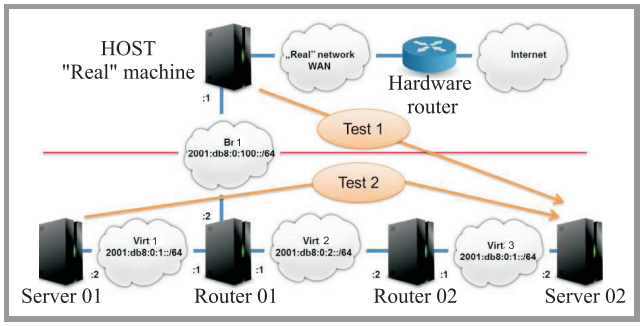


Fig. 11. The test of the static routing.

7.4. The Automatic Address Configuration Tests

The purpose of the tests is to check the functioning of the automatic configuration of the network interface addresses. Three methods of configurations were tested and results are presented: the stateless addressing, the stateful addressing and the configuration through the relay agent. The tests check the readiness of the virtual environment and the virtual machines based on MS Windows server 2008 R2 to the migration processes. If the automatic address configuration is carried out correctly, there is no need to configure manually the network interfaces on the new host machine after the migration process. The configuration of the test environment is presented in Fig. 12.

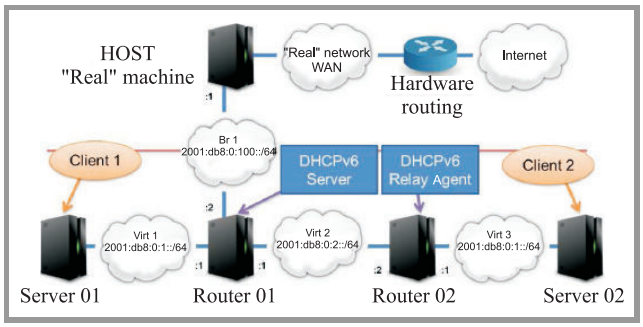


Fig. 12. The test environment for the automatic address configuration.

7.5. The Stateless Addressing Test

The stateless address configuration is very convenient if any sophisticated parameters have not to be configured on the network interface and a quick and easy method of configuration, without administrator intervention, is demanded. A computer which interface is to be configured is called the client. The stateless configuration is the process in which the client interface is configured to obtain the IPv6 address automatically and the configuration process is based on the exchange of messages between the client computer and the router in the network the interface is connected to. There is no DHCP server. Server 01 as the client (Client 1 in Fig. 12) and Router 01 as the router to exchange messages were configured in the test. It was expected, that client would be configured with the unique IPv6 address and the default gateway. The DNS server addresses are configured automatically as fec0:0:0:ffff::1%1, fec0:0:0:ffff::2%1, fec0:0:0:ffff::3%1. The initial configuration of the client interfaces is shown in Fig. 13.

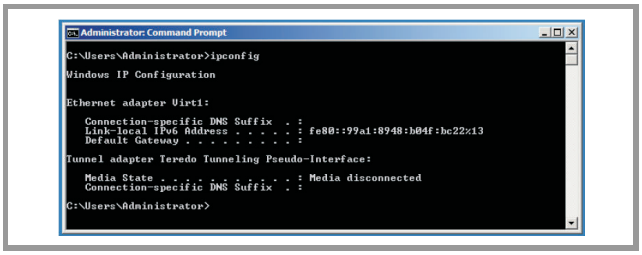


Fig. 13. The initial configuration of the client interfaces.

The interface Virt 1 was configured. After configuration process, the client was correctly configured and the check of connectivity was carried out. The default gateway was configured as the link-local address. There were no issues with the stateless addressing.

7.6. The Stateful Addressing Test

The stateful configuration can be used for more sophisticated configuration of the network interface, where the stateless configuration is insufficient and/or we want to reserve addresses. The DHCP service is used to configure clients. In the test environment Router 01 was configured as the DHCP server and Server 01 acted as the client (Fig. 12). It was expected, that the client would be configured by the DHCP server with the IPv6 address, the address of the DNS servers and the DNS domain the machine belongs to. The default gateway would be configured by the router. Both cases of address selection were tested: any address from the scope and the reserved.
The DHCP server was configured with the scope with the following parameters:

- the network prefix: 2001:db8:0:1::/64,
- the excluded addresses 2001:db8:0:1:: to 2001:db8:0:1::ffff,
- the DNS server address: 2001:db8:0:100::1.

Since the DHCP server is the router, the advertisements of the default rout ware enabled:

- netsh interface ipv6 set interface Virt 1 advertisedefaultroute=enabled,
- netsh interface ipv6 set interface Virt 1 advertise=enabled The reservations of IPv6 addresses were performed.

During the test, the client was correctly assigned all the demanded parameters. The default gateway was configured as the link-local address. There were no communication issues.

7.7. The DHCP Relay Agent Test

The DHCP relay agent test has the same assumptions as stateful addressing test, but additionally we assume that

the DHCPv6 server is not connected to the subnet of the client and the realy agent is demanded between client and the DHCP server. In this test, Server 02 act as the client (Client 2) and Router 02 is configured with the relay agent role (Fig. 12). The relay agent was configured as in Fig. 14.

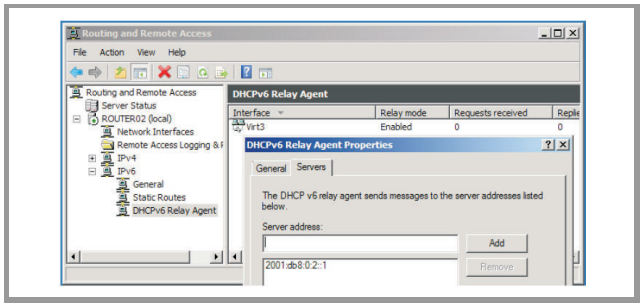


Fig. 14. The relay agent configuration.

Additionally, the options advertise, advertisedefaultroute, managedaddress oraz otherstateful should be enabled for the Virt 3 interface on Router 03. The client was configured correctly.

7.8. The DNS Integration Test

The client computers and virtual machines can register itself in their DNS domain without the intervention of the network administrator. The DNS integration test consists of checking the registration process. This feature facilitates the migration of virtual machines. If that process works correctly, we can assume, that even the IPv6 address changes during the migration process, we can still contact the migrated machine via the fully qualified domain name which remain unchanged and is correctly translated to the current client machine IPv6 address by the DNS server.
The corporate model of the MS Windows implementation assumes operations in Active Directory for the security reason. During the integration test, it was stated that the virtual machines have to join the Active Directory domain for proper registration in DNS domain. There were no problems with the self-registration process in DNS.

8. Conclusions

The results of tests conducted for the Hyper-V virtualizer can be summarized as:

- The Hyper-V virtualization environment and MS Windows 2008R2 server (tested on enterprise edition) in the role of the host and the virtual machines, working exclusively with IPv6, behave properly with addresses assigned statically and dynamically (including stateless and stateful configuration). There is no issues with manually configured routing.
- There are no communication problems at the border of the host computer (host) and virtual machines (guests).
- MS Windows 2008R2 server used in the proposed testing environment does not support dynamic routing, therefore dynamic routing has not been tested.

As a second step of presented research the experiments of Hyper-V virtualizer will be conducted using experimental network that consists of two physical servers Server1 and Server 2 combining different virtual entities representing intranet connections and a physical Switch 1 to communicate between the two physical servers. All the virtual network traffic is multiplexed over the physical 10/100/1000 Mbit/s Ethernet interfaces of Server 1 and Server 2.

Acknowledgement

The research presented in this paper has been partially supported by the European Union within the European Regional Development Fund program no. POIG.01.01.02-00-045/09-00.

References

[1] Y. Mun and H. K. Lee, *Understanding IPv6*. New York: Springer, 2005.

[2] *An IPv6 Deployment Guide*. M. Dunmore, Ed. The 6NET Consortium, Sept. 2006.

[3] I. van Beijnum, *Running IPv6*. Berkeley: Apress, 2005.

[4] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification". RFC 1883 (proposed standard), obsoleted by RFC 2460, IETF, Dec. 1995.

[5] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification". RFC 2460 (draft standard), updated by RFCs 5095, 5722, 5871, IETF, Dec. 1998.

[6] J. Postel, "Internet protocol". RFC 791 (standard), updated by RFC 1349, IETF, Sept. 1981.

[7] R. Gilligan and E. Nordmark, "Transition mechanisms for IPv6 hosts and routers." RFC 2893 (proposed standard), obsoleted by RFC 4213, IETF, Aug. 2000.

[8] B. Carpenter and C. Jung, "Transmission of IPv6 over IPv4 domains without explicit tunnels". RFC 2529 (proposed standard), IETF, March 1999.

[9] F. Templin, T. Gleeson, and D. Thaler, "Intra-site automatic tunnel addressing protocol (ISATAP)". RFC 5214 (informational), IETF, March 2008.

[10] C. Huitema, "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)". RFC 4380 (proposed standard), IETF, Feb. 2006.

[11] B. Carpenter and K. Moore, "Connection of IPv6 domains via IPv4 clouds." RFC 3056 (proposed standard), IETF, Feb. 2001.

[12] N. Wang *et al.*, "A framework for lightweight QoS provisioning: Network planes and parallel internets", in *Proc. 10th Int. Symp. on Integrated Network Management*, IEEE, 2007, pp. 797–800.

[13] J. Kwiatkowski, M. Pawlik, M. Fras, M. Konieczny, A. Wasilewski, "Design of SOA-based distribution system", in *SOA Infrastructure Tools – Concepts and Methods*, Poznań University of Economics Press, 2010, pp. 263–288.

Krzysztof Chudzik – for biography, see this issue, p. 12.

Jan Kwiatkowski – for biography, see this issue, p. 13.

Paper

IPv6 in Wireless Networks – Selected Issues

Sławomir Kukliński[a], Paweł Radziszewski[b] and Jacek Wytrębowicz[b]

[a] Institute of Telecommunication, Warsaw University of Technology, Warsaw, Poland
[b] Institute of Computer Science, Warsaw University of Technology, Warsaw, Poland

Abstract—The article presents issues concerning the construction of autonomous wireless networks based on the IPv6 protocol. Prospects of implementation of IPv6 in wireless networks and IPv6 features and mechanisms important in such applications are discussed. Research directions related to the use of IPv6 in wireless networks are also outlined. Then the selected concepts are described, arising in the course of the EFIPSANS (Exposing the Features in IP Version Six Protocols that can be Exploited/Extended for the Purposes of Designing/Building Autonomic Networks and Services) project, during studies on the autonomy of nodes and routing configuration for wireless networks. Concepts presented here apply to wireless ad hoc mesh networks. Discussed is their nature and aspects related to auto-configuration and autonomously operating routing. In particular, there is a Wireless Autonomic Routing Framework (WARF) architecture presented.

Keywords—extension headers, IPv6, WiFi, wireless mesh networks.

1. Introduction

Techniques for creating wireless networks for data transmission are as old and complex as those dedicated to wired ones. Observing the development of wireless networks over the past 40 years, two seemingly contradictory trends can be found: high specialization towards a particular application and uniformity in order to open for application software and to connect globally available subnets to the network. This is an apparent contradiction, because the first goal is achieved by choosing and developing the layer 2 protocols, while the second objective is achieved by applying the higher layers of TCP/IP protocol stack. Today many different types of wireless networks are used, such as:

- mobile communication networks, like CDMA2000, EDGE, UMTS and LTE;
- private radio networks built using TETRA and GSM-R technologies;
- broadband access networks exploiting WiMAX (IEEE 802.16) and WiFi (IEEE 802.11) technologies;
- nomadic and mobile ad hoc networks relying on WiFi;
- sensor networks exploiting ZigBee (IEEE 802.15.4) technology.

They differ not only in layer 2 protocols. Their diversity is derived from the application requirements, geographical coverage, number and mobility of nodes. The prevalence of their deployments is also driven by economic factors (including the history of the development of local economies) and cultural aspects, resulting from the degree of education of local communities.

Most of today's wireless networks use the IPv4 protocol, adopted as a mandatory standard in 1981 (RFC 791). Its widespread use was 10 years later, when first web servers and web browsers appeared. IPv6 was adopted as a standard in 1998 (RFC 1883) and its global availability is possible only since February 2008, when IANA launched IPv6 DNS servers in the Internet backbone. The number of devices using IPv4 is huge and difficult to assess because of the countless number of private networks and the widespread use of NAT. It is difficult to expect that, in a short term, users of these devices decide for their replacement or reconfiguration in order to move to IPv6. It is also probable that, despite the many advantages of IPv6, majority of the current IPv4 users will not want to change, assessing that their network infrastructure meets their needs. On the other hand, the pool of free IPv4 addresses is running out. On the basis of automatically updated statistics (IPv4 address report[1]) it can be concluded that (at the time of writing this publication):

- number of IANA- and RIR-alocated public IPv4 addresses is 3 098 000 000;
- number of public IPv4 addresses observed in core routers' BGP tables is 2 236 000 000;
- exhaustion of free IANA-allocatable address pool will happen on July 19th 2011;
- exhaustion of free RIR-allocatable address pool will happen on March 25th 2012.

At present we see that the global Internet is single, supported parallelly by two protocols: IPv4 and IPv6. Therefore, we can be sure that due to the depletion of free IPv4 addresses, new installations of Internet access networks will be based on IPv6. However, the rate of the existing networks modification will result from the emergence of new applications and network services, which functionality will depend on the version of the IP protocol.

IPv6 compared to IPv4 has several advantages, as it formed on the basis of experience of the operation of IPv4 networks. The benefits of deploying IPv6 are discussed in many publications, e.g., [1], [2], [3], [4]. What is worth

[1] www.potaroo.net/tools/ipv4/index.html

to emphasize, this protocol is pro-developmental in terms of ease of creating new technical solutions and new-quality applications. It is possible to increase the globalization of remote data collecting and control, in relation to the massive amount of terminal equipment. This also applies to the access to devices operating in wireless networks.
There also several books written on the use of IPv6 in wireless networks, e.g., [5], [6]. In summary, it can be concluded that the IPv6 features important for the provisioning of services in wireless networks, are:

- The size of the address space, important for operators servicing millions of subscribers.
- Powerful mobility, which allows nodes to move between subnets without breaking the existing session. Mobile IPv6 is more efficient than Mobile IPv4. With Mobile IPv6 a number of enhancements is related, such as hierarchical management of nodes mobility (RFC 5380), subnet mobility within the Internet (RFC 3963), rapid transfer of nodes between access routers (RFC 5568) using layer 2 mechanisms (e.g., WiFi roaming, WiMax), routing optimization (RFC 4866), possibility of take-over of the responsibility for the signaling associated with the node mobility (RFC 5213) by the network.
- Auto-configuration features are enhanced (detection of neighbors and routers, announcing the network prefix).
- The use of header compression potentially makes IPv6 more efficient than IPv4 – which is particularly important in sensor networks.
- IPv6 offers higher level of security compared to IPv4, because
  - a mandatory implementation of IPsec provides more options for securing networks and applications - without the constraints imposed by NAT servers;
  - there is defined a proposal of a standard for securing, with IPsec and IKEv21, the signaling between mobile nodes and home agents (RFC 4877);
  - it is possible to use the Secure Neighbor Discovery Protocol (SEND, RFC 3971), which improves the safety of nodes auto-configuration – which is particularly important in the radio interfaces;
  - SEND protocol increases the security of neighbors discovery process. It's most important mechanisms are certification paths for routers authentication, and cryptographically generated addresses (RFC 3972) to verify the sender.
- There is possible interoperability of devices in IPv6 and IPv4 subnets and tunneling of IPv6 traffic in IPv4 subnets.

Noteworthy is an interesting study [7] of the use of IPv6 in the satellite communication, commonly used in military applications and for multimedia content distribution (e.g., IPTV). Features typical in satellite communications, such as broadcast and multicast, mobility and global reachability, are well supported by IPv6.
Today, ongoing research related to wireless networks and IPv6 protocol addresses a number of very different issues. Deserve a mention works on:

- communication between devices with low power consumption, led by 6lowpan Working Group (IETF);
- optimization of Mobile IPv6 solutions, led by MobOpts Working Group (IETF);
- communication between cars, and cars and road infrastructure in order to increase road safety (Geonet Project, 7th Framework Programme);
- autonomy of the nodes and networks within the aforementioned project EFIPSANS.

Issues that were analyzed in the EFIPSANS project were: ISO/OSI crosslayer cooperation to improve the performance of a wireless network [8], multipath routing, which can increase performance and reliability of the network [9], [10], mechanisms that can force node users to a cooperation in order to optimize the utilization of network resources [11], [12]. The result of the work is the WARF architecture, presented later in this article, designed to support autonomous routing in wireless mesh networks. In the last section there is a concept of a new IPv6 extension header presented, which is a solution for an efficient transport of auto-configuration and routing messages within the wireless network.

2. Routing in Wireless Mesh Networks

Our interest focuses on wireless ad hoc networks, built on the basis of a popular IEEE 802.11 standard. The popularity is due to the extremely low equipment prices and very attractive operating parameters [13], such as working in unlicensed radio bands, high resistance to interferences, high transmission rates. Ad hoc networks are a hot topic of research for over 10 years. Approximately 120 routing protocols for such networks were proposed, but prior to the publication of the IEEE 802.11 standard in 1997, existed only 6 of them. Most of these proposals were published in the conference materials, 30 of them were proposed IETF standards, 2 of them are active IETF proposals and 4 have become the IETF standards. Furthermore, there are 4 patented proprietary protocols offered in commercial solutions. The multiplicity of these protocols demonstrates the conflicting requirements of different applications of such networks. Mobile ad hoc networks are the subject of multiple present scientific conferences, such as *Ubi-Islands, International Conference on Ad Hoc Networks, In-*

ternational Conference on Cognitive Radio Oriented Wireless Networks and Communications, ICST Conference on Access Network, International Conference of Wireless Networks, IEEE Symposium on Personal, Indoor and Mobile Radio Communications.

A variation of ad hoc networks with relatively low topology variability is a wireless mesh networks (WMN). WMNs can be created as residential area networks, interim solutions for servicing events, etc. They assume so-called nomadic nature of users, namely the lack of mobility while using the network. WMNs are typically created using nodes with IEEE 802.11 radio interfaces. Despite years of research, deployment rates of such networks are still very low. A cause is that not all the problems associated with such networks have been solved. There were too many routing protocols developed, each of which has beneficial properties only in a specific network scenario: some protocols work efficiently in networks with low or high density of nodes, while the other ones are dedicated to networks with low or high topology changes dynamics. Unfortunately, in many WMN applications it is difficult to assume the characteristics of network environment. The problem of selecting an appropriate network protocol is further reinforced by the ambiguous evaluation of the effectiveness of metrics used by the routing protocols (usually they are part of the routing protocols). A number of metrics specific to the WMNs (including ETX, ETT, Airtime [14]) had been developed, initial implementations, however, have not confirmed the benefits of certain metrics, indicated by simulations [15].

One of the problems of present WMN solutions is the lack of information exchange between different network layers. Such an approach significantly and adversely affects the network behavior. A glaring example is the use of routing protocols, which choose a path with the least number of intermediate nodes (hop-count metric). In practice, it appeared that a path formed in this way chooses the longest network spans and therefore the ones characterized by the lowest SNR, and consequently low bitrate (bitrate adaptation to the link quality is part of the IEEE 802.11 standard) and the high probability of packet loss (packet loss rate parameter) [16]. Using information from the physical layer would reject low-quality links in such a case. It is worth noting that the use of information from different layers (cross-layer) is a classical approach used in mobile communication systems (GSM/UMTS/LTE). In IP networks such an approach is still not popular. Another problem of 802.11 mesh networks is that all nodes of the network use the same radio channel. This leads to poor network performance due to the formation of relatively large 'areas of interference', where only one node can transmit at the same time.

Furthermore, in most WMNs network management is still centralized, inadequate to the possibility of spontaneous division of the network into two disjoint networks or a combination of two disjoint networks into one. WMNs require specific network management solutions with special focus on auto-configuration (including IP address allocation). WMN networks are usually created not by the operators with relevant experience, but by small companies or the network users themselves. So an important requirement is to incorporate the advanced autonomous management functions into them; manual management should be kept to a minimum.

3. Auto-configuration in Wireless Mesh Networks

Wireless networks, because of their usually higher topology variability, can much more benefit from the auto-configuration features than wired networks. Therefore, IPv6 can be preferred over IPv4, having more support for auto-configuration.

There are two kinds of auto-configuration in IPv6:

- stateful – similar to that known from IPv4, using DHCPv6 servers;
- stateless – that does not require the use of such servers (RFC 2462).

A particular attention deserves the stateless auto-configuration, occurring in IPv4 only in a rudimentary form – dynamic configuration of IPv4 link-local addresses (RFC 3927) and automatic private IP addressing and allocating for communication purposes local addresses from the range 169.254.0.0/16. The most important mechanisms for stateless auto-configuration of IPv6 are: link-local addressing, automatically generated interface IDs, neighbor discovery, duplicate address detection, router discovery and prefix announcement.

IPv6 defines several validity ranges of the addresses, from which the most important are global and link-local addresses. Global addresses are equivalent to public IPv4 addresses and can be used across the public Internet. Link-local address is valid and must be unique only in the "link", understood as a layer 3 network. IPv6 allocates prefix FE80::/10 for this purpose. These addresses allow for communication between devices within the same network, without having any knowledge of their location in the surrounding networks, and so the network prefix. They can be defined manually, but most are generated automatically, from layer 2 addresses, using the EUI-64 (extended unique identifier) schema. This allows for an easy connectivity setup between devices attached to the same network.

As IPv6 does not define a broadcast address, it is impossible to use well-known IPv4 ARP. It is replaced by the neighbor discovery mechanism, supported by duplicate addresses detection, which are part of the ICMPv6 protocol. IPv6 allows the end device that use the ICMPv6 protocol for an automatic detection of the default router and the announcement of the network prefix. In conjunction with the automatic generation of the interface ID it allows to automatically configure a full IPv6 address (64-bit network prefix and 64-bit interface identifier), which provides communication between different networks.

The research in the EFIPSANS project has defined new mechanisms to support auto-configuration of wireless networks – the use of several radio interfaces, automatic allocation of radio channels and multi-path routing. For transport of auto-configuration messages IPv6 mechanism of the extension headers is used. It allows to attach control messages to user traffic packets, which is especially advantageous in radio networks with multiple access to a shared medium, due to lack of efficiency losses as a result of additional packets competing for access to the transmission channel.

4. WARF Architecture

The above-mentioned problems associated with WMNs show that a new, open and comprehensive approach to such networks is necessary. It should:

- provide a distributed, autonomous management mechanisms;
- facilitate exchange of information between the layers of the network stack;
- support simultaneous use of different routing protocols (multi-protocol approach);
- allow for the multipath routing;
- ensure the determination of routing metrics in a routing protocol-independent way;
- allow the creation of networks using nodes with multiple radio interfaces.

Above requirements are met by the wireless autonomic routing framework (WARF) architecture, developed by the authors of this article in the aforementioned EFIPSANS project. The main idea of the WARF approach is to create an open environment for WMNs, supporting the abovementioned, advanced mechanisms, allowing for a relatively easy replacement of algorithms responsible for each specific functionality. WARF is component architecture, allowing for flexibility in the implementation of various routing protocols, routing metrics and radio resource management mechanisms. The use of multiple radio interfaces enables the dynamic resource (radio channels) management mechanism. It must be, however, supported by an appropriate control protocol.

The WARF architecture defines basic building blocks responsible for realization of specific functions. Control messages exchange is performed by the IPv6 protocol, which offers significant benefits like large address space, mobility support and automatic protocol configuration, with additional features called WARF extensions. Thanks to the unified approach to control messages transport it is possible to interpret different messages by all WARF network nodes. One of the mechanisms used for the unified message transport mechanism is IPv6 WARF extension header. The presented mechanisms contribute to higher level of autonomy of the management of such networks, increasing their productivity and reliability, as well as facilitating implementation. WARF extensions can be also used to encapsulate control messages of existing routing protocols such as AODV or AOMDV.

WARF architecture decomposition into functional blocks results from a comparative analysis of ad hoc networks/WMNs routing protocols and the specifics of new, described above, routing and resource management mechanisms. The proposed decomposition is consistent with the autonomous model proposed by IBM [17]. In this model stands out: a part collecting information about the status of the module or a network node (a sensory part), a decision component (which in fact contains a control algorithm and a knowledge base) and actuators. Due to the impact of the decision on the status of the network and feedback information obtained from sensors, we are dealing with a system with feedback, with all the consequences of it – among others the possibility of a delayed action or unstable operation of a node, subnet or a whole network.

WARF architecture is similar to the decomposition proposed by [18]. It consists of four main blocks, divided further into modules (see Fig. 1):

- Resource Maintenance (RSM),
- Route Maintenance (RTM),
- Data Forwarding (DF),
- Policy Control (PC).

Resource Maintenance block contains a Resource State Information (RSI) and a Resource Control (RC) modules.

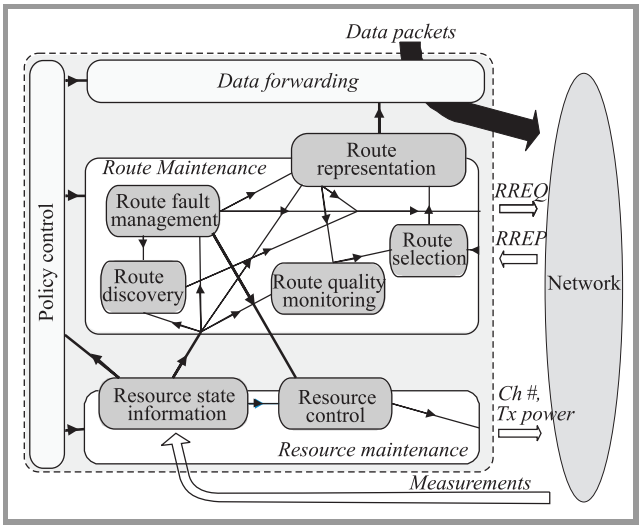


Fig. 1. WARF architecture: Route Maintenance block consists of 4 modules: route discovery, route selection, route representation and route fault detection.

The RSI module is responsible for radio resources (channels, radio links) monitoring – it monitors and spreads all the information related to the resources state. This may include parameters of different network layers, including SNR/SNIR, BER, FER, PLR, node load level, etc.

Table 1
WARF architecture signalling messages

Category	Message	Parameters
Radio resource control	Channel quality report (CHQREPORT)	Number of radio channels Channel ID SNR Channel load Reporting node IPv6 address
	Number of interfaces report (INTFREPORT)	Number of interfaces Interface ID Channel ID, TX power Rporting node IPv6 address
	Set signalling channel (SETSIGHCH)	Channel ID, TX power Requesting node IPv6 address Target node IPv6 address
Route control	Path metric (PATHMETRIC)	Packet error rate, bit error rate Retransmission count Delay, delay variance Bit rate Announcing node IPv6 address Destination network IPv6 address and mask
Legacy routing protocol support (AODV)	IPv6 route request (PREQ) Route reply (RREP) Route error (RERR) Route reply acknowledgment (PREP-ACK)	Parameters analog to the ones from the original AODV protocol, adopted for transporting IPv6 address information instead of IPv4

This module monitors both used and available resources. This is important because of the adaptability of link parameters to propagation conditions. All these operations are performed in real time. RSI may perform measurements aggregation before further information transfer. This module supports also calculations of routing metrics.

Resource control module is responsible for radio resource configuration. The algorithm controlling its operation uses the RSI module information (quality of links and their load) and on this basis decides whether to change the configuration of resources. Reconfiguration may be due to a congestion in the selected routes or a damage to the links. To change the configuration of a radio channel a three-way handshake protocol is used, and signalling messages are have form of IPv6 WARF extension headers.

These modules work together to create a routing table, which is the main output product of this block. They use the resource configuration and state information in order to obtain information about the quality of paths (metrics). All external information of this block use the same IPv6 WARF extension, regardless of the algorithm (routing protocol) used. When in this block classic protocols are used, signalling messages are simply encapsulated. WARF messages of this block are classic routing protocols messages, such as RouteREQest (RREQ), RouteRESPonse (RRESP), RouteERRor (RERR).

Data forwarding block uses a routing table to forward packets. It selects the paths based on metrics. In the WARF architecture it is assumed that this block can support multipath routing and QoS mechanisms, but these operations require no additional WARF control messages. There is also no support of flows at the signalling level. Such support, however, can be built in.

Policy Control block controls all other blocks and modules. WARF is architecture with elements of autonomous administration and a number of parameters of this architecture are subject to self-regulation. Nevertheless, it has been decided to leave some degree of freedom, allowing the network operator to create different policies or change the network profile. The policy control block provides such mechanisms.

5. IPv6 WARF Extension Header

In the described approach, it is proposed to use IPv6 protocol extension headers (RFC 2460) as a channel for transporting WARF architecture signalling messages. WARF-aware nodes can attach these messages as an additional extension header, of the hop-by-hop option category, to user data packets. Header of this category is being analyzed by all the nodes along the packet path. Such an approach has an important advantage: it does not generate additional packets, what decreases demand for computing power in communicating nodes and, what is especially important in wireless networks, does not load the transmission channel with the process of the medium access competition.

Signalling messages, encapsulated in IPv6 extension header are forwarded between nodes. There is proposed a hop-by-

hop header, with number from the range 32-63. It's leading bits (001) mean "skip the header when you not recognize it" (assuring compatibility with non-WARF-aware nodes) and "a header can change along the path".
Structure of the proposed header fulfills the RFC 2460 requirements. One header can transport multiple messages. Messages are grouped into three categories: radio resource control, routing control and support for the legacy routing protocol (e.g., AODV). Their list is presented in Table 1.
One should be aware of two potential disadvantages of sending messages via extension headers:

- It increases data packets length; it can excess the MTU value for the given network.
- When no user data is sent for some time, an unacceptable delay in the signalling messages delivery can occur.

Countermeasures to these shortcomings are easy to design. It is proposed to use for the control messages transport only short packets (e.g., TCP acknowledgement messages or UDP voice packets). Moreover, it is possible to implement an integrated, intelligent transport, which, depending on the occurrence and character of the user data and signal message urgency, selects for it's transport one of three channels: extension header, ICMP packet or zero-payload packet.

6. Conclusions

The use of IPv6 in the Internet is now a reality. We are observing a rapid development of dedicated IPv6 extensions for mobile applications and wireless networks. The essential features of IPv6 and its extensions in support of the construction and operation of wireless networks are mechanisms for mobility, auto-configuration and security.
Presented in this article some results of studies carried out in the EFIPSANS project show that deployment of a new extension header can effectively support the operation of wireless mesh ad hoc networks. In particular, it can improve routing mechanisms.
Although theoretical work on the operation of ad hoc mesh networks is being carried for several years, their widespread use is limited. The reason for this is twofold: lack of applications due to lack of universality of such networks and lack of universality due to lack of autonomy of routing configuration. Routing algorithms and their parameters should be selected to the specifics of the installation and use. This requirement can be met through the deployment of WARF architecture.
We think that the proposed IPv6 extension header could become a factor facilitating construction of flexible routing architecture for wireless ad hoc networks and consequently make them more efficient and effective in supporting a variety of applications. Although IPv6 is not being implemented in existing networks as quickly as expected, we are convinced that in a few years it will be widely used. A steady increase in the number of applications and services that require a constant visibility of each node in a network can be observed. For such applications and services a direct visibility of the nodes, node independence and continuity of network access are key features. As IPv6 better than IPv4 meets these objectives, it is deployed in new networks and will, with some delay, appear in the existing ones.

References

[1] R. Desmeules, "Cisco self-study: implementing Cisco IPv6 networks (IPV6)". *Ciscopress*, 2003.

[2] S. Hagen, *IPv6 Essentials*. O'Reilly, 2006.

[3] K. Siil, *IPv6 Mandates: Choosing a Transition Strategy, Preparing Transition Plans, and Executing the Migration of a Network to IPv6*. Wiley, 2008.

[4] M. Blanchet, *Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks*. Wiley, 2006.

[5] H. Soliman, *Mobile IPv6: Mobility in a Wireless Internet*. Addison-Wesley Professional, 2004.

[6] R. S. Koodli, Ch. E. Perkins, *Mobile Inter-networking with IPv6: Concepts, Principles and Practices*. Wiley, 2007.

[7] D. Minoli, *Satellite Systems Engineering in an IPv6 Environment*. Auerbach Publications, 2009.

[8] R. Ramdhany, G. Coulson, "Manetkit: a framework for MANET routing protocols", Lancaster University UK, 2010 [Online]. Available: http://www.comp.lancs.ac.uk/≈geoff/Publications/WWASN2008.pdf

[9] M. K. Marina, S. R. Das, "On-demand multipath distance vector routing in ad hoc network", in *Proc. ICNP 2001*, Riverside, USA, 2001, pp. 14–23.

[10] S.-J. Lee, M. Gerla, "Split multipath routing with maximally disjoint paths in ad hoc networks", in *Proc. IEEE Int. Conf. Commun. ICC'01*, Helsinki, Finland, 2001, vol. 10, pp. 3201–3205.

[11] P. Michiardi, R. Molva, "CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks", in *Proc. Commun. Multim. Sec. Conf.* Portoroz, Slovenia, 2002, pp. 107–121.

[12] S. Buchegger, J.-Y. Le Boudec, "Performance analysis of the CONFIDANT protocol: cooperation of nodes fairness in dynamic ad hoc networks", in *Proc. MobiHoc'02*, Lausanne, Switzerland, 2002, pp. 80–91.

[13] E. Perahia, R. Stacey, *Next Generation Wireless LANs: Throughput, Robustness, and Reliability in 802.11n*. Cambridge University Press, 2008.

[14] R. Baumann, S. Heimlicher, M. Strasser, A. Weibel, "A survey on routing metrics", TIK Report 262, *ETH* Zürich, Feb. 2006.

[15] H. Ştefănescu, M. Skrocki, S. Kukliński, "AAODV routing protocol: the impact of the routing metric on the performance of wireless mesh networks", in *Proc. 6th Int. Conf. Wirel. Mob. Commun.*, Valencia, Spain, 2010.

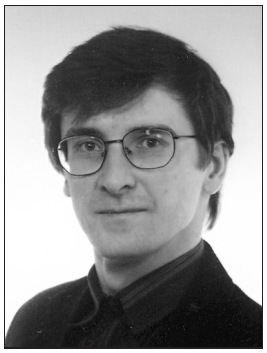
[16] D. Passos, D. V. Teixeira, D. C. Muchaluat-Saade, L. C. S. Magalhães, C. V. N. Albuquerque, "Mesh network performance measurements", in *Proc. 5th Int. Inform. Telecommun. Technol. Symp.*, Cuiabá, Brazil, 2006.

[17] IBM, "Autonomic Computing White Paper: An architectural blueprint for autonomic computing", 4th edition, June 2006 [Online]. Available: http://www-01.ibm.com/software/tivoli/autonomic/pdfs/AC_Blueprint_White_Paper_4th.pdf

[18] I-J. Wang, J. Hopkins, Ch. Liu, T. Saadawi, "Component-based analysis and design of routing protocols for mobile ad hoc networks", 2005 [Online]. Available: http://handle.dtic.mil/100.2/ADA431954

Sławomir Kukliński received Ph.D. degree in telecommunications from Warsaw University of Technology, Institute of Telecommunications in 1994 and since then he is a Professor. He has 25 years long experience in telecommunications – he started from radar systems, switched to distributed algorithms for signal processing (including neural networks) and from 10 years he is working on mobile and wireless systems. At WUT he is a lecturer of mobile systems. In 2003 he joined the Orange Labs Poland. In Orange Labs Poland he is involved in projects related to autonomic management and VANET (car-to-car communications). He was recently involved in FP6 MIDAS project working on context aware routing. Since 2008 he is involved in FP7 project EFIPSANS. In 2008 he has started another project, AUTONET (Autonomic, Wireless Networks) that has been ordered and is financed by Polish Ministry of Science and Higher Education. From January 2008 till July 2010 he was involved in FP7 project 4WARD. He published more than 40 papers, and he also was the member of TPC of many conferences and served as a reviewer to many conferences and journals.

e-mail: kuklinski@tele.pw.edu.pl
Institute of Telecommunication
Faculty of Electronics
and Information Technology
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland



Paweł Radziszewski received M.Sc. (1993) in computer science from the Faculty of Electronics and Information Technology, Warsaw University of Technology. Since that he works at the Institute of Computer Science, WUT. His research interests include: computer networks (especially network protocols and network steganography), software engineering and computer graphics. He is member of Computer Graphics Laboratory. He is an author or a co-author of 10 papers. Since 1993 he has been working as a software developer for TecMath GmbH (Germany), Softwired A.G. (Switzerland), Arkatronik (Poland) and Air Force Institute of Technology (Poland). Since 2003 he has been working as an instructor at the Cisco Regional Academy at International Telecommunication Union Internet Training Centre, WUT. In years 2007–2008 he was involved in the TrustMAS project concerning steganographic routing. Since 2008 he is involved in FP7 project EFIPSANS.

e-mail: p.radziszewski@ii.pw.edu.pl
Institute of Computer Science
Faculty of Electronics
and Information Technology
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

Jacek Wytrębowicz is an assistant professor at Warsaw University of Technology, where he gives lectures on computer networks. He is co-author of 4 books and author or co-author of 35 papers in technical journals and conference proceedings. When he worked at Warsaw Heating Utility, he led a project of a Metropolitan Area Network. During this time the company built 50 km of fiber infrastructure inside heat distribution ducts. Working at TEL-ENERGO S.A. (today named EXATEL S.A.) a countrywide telecom operator, he managed the IT department and was responsible for development of business and operational support systems. He is a specialist in Internet protocols and triple play services. As a consultant he wrote technical analysis and telecommunication strategies for municipal authorities and utility companies from Warsaw and Torun. He has a Ph.D. in Computer and Network Science from l'Ecole Nationale Supérieure des Télécommunications Paris and M.Sc. in Computer Science from Warsaw University of Technology.

e-mail: j.wytrebowicz@ii.pw.edu.pl
Institute of Computer Science
Faculty of Electronics
and Information Technology
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

Paper

On Implementing IPTV Platform with IPv4 and IPv6 Devices

Jordi Mongay Batalla[a,b] and Piotr Krawiec[b]

[a] National Institute of Telecommunications, Warsaw, Poland
[b] Warsaw University of Technology, Warsaw, Poland

Abstract—The end of IPv4 addresses is now a reality. Providers not updated to IPv6 will have to hurry up the IPv6 start in its own network. Introduction of IPv6 means not only change of main routers but also change of mentality in operators, applications' programmers besides end users. Even when for the last years the core network is prepared for transferring IPv6 traffic, other built-in parts of the Internet limit the IPv6 start. Examples of these limitations we find in not IPv6-awareness of many applications and services. For instance, voice over IP service, which uses session initiation protocol (SIP) needs to implement IPv6 aware SIP proxies and IPv6 aware AAA (authentication, authorization and accounting) servers as well as adapting application programming interfaces to IPv6. Internet protocol television (IPTV) system includes many different hardware devices, which not always are IPv6 compatible. In this paper, we propose a global solution for integrating all the devices, these one working on IPv4 and these one working on IPv6, under the same IPTV platform. This solution allows end users to receive IPTV stream irrespective of IP protocol used. The proposed solution is particularly relevant for small IPTV systems, which, step by step, are adapting into IPv6.

Keywords—"good practices", IPTV, IPv4/IPv6 interoperability, IPv6, set top box.

1. Introduction

Is IPv6 here already? It seems difficult to answer to this question. For sure IPv6 is arriving for the last 20 years. Mistrust of operators and companies are justified. ICT'2010, one of the most important *Information and Communication Technologies* conferences in Europe organized by the European Commission, presented the current state of implementation of IPv6 in Europe, and the future of IPv6 in Europe does seem overcast; on the one hand the IPv4 addresses are really finishing: deadline is 2012; on the other hand there are several steps missing for total operation of IPv6 all around Europe, and the countries, which will not work with IPv6 risk incomplete operation within a near future.

Building a network fully IPv6-aware comes up as a difficult task because Internet protocol is related with all the systems and devices (horizontal point of view), and at the same time it is the bottleneck of the layer architecture of the Internet (known as hour-glass model of the Internet). The hour-glass model implies that almost all the layers of the network have to do with the Internet protocol (vertical point of view).

From a horizontal point of view, all the systems of the network as, e.g., multimedia systems, distributed databases, even tester platforms [1] should adapt to IPv6. By bringing into operation IPv6 in entire systems as network services the IPv6 traffic increases within the network. For example, Google activated IPv6 in internal Youtube communications, increasing in this way the IPv6 traffic in the Internet up to 3000% [2]. Google needs IPv6 to build all the offered services inside one unique network, which is a requirement of the business plan. Other large systems in the Internet as, e.g., Yahoo and Facebook are actually starting on IPv6. Akamai[1] has just also announced IPv6 start.

Not only larger and universally extended service systems in the Internet must overcome different troubles for IPv6 start, but also the small systems find different difficulties during this process. Notice that small systems have much fewer economic resources for starting IPv6.

In this paper, we analyze the IPv6 start for Internet protocol television (IPTV) centering in the emerged problems when we set in motion IPTV system over devices, some working on IPv4 and some of them working on IPv6. We propose a solution based on sending to the network two parallel multicast streams, each one for one IP protocol (v4 and v6). To double the IPTV stream, we consider two independent networks and locate a server (IPv4/IPv6 server), which transmits between IPv4 and IPv6 "zones". This server is able to receive multicast flows generated by IPv4 devices and resend them in IPv6 multicast transmission to the IPv6 hosts. It can also perform transmission in opposite direction, when the IPTV signal source is located in IPv6 network and the destination is in IPv4 domain.

Let us remark that classical translation mechanisms are not useful in considered IPTV scenario, since multicast addresses may not be simply translated. The shortcoming of the proposed solution may derive from the effectiveness of the IPv4/IPv6 server in case of resending TV streams with high capacity.

The paper is structured as follows. In the next section we present the overview of the IPTV system that we tried to migrate to IPv6. Then, we describe the solution for IPv4/IPv6 environment. After that, in Section 4 we show the results of effectiveness study for proposed solution and conclude the paper in Section 5.

[1] www.akamai.com

2. Overview of the IPTV System

Multimedia communications are crucial for the definitive supremacy of packet networks over other connecting platforms. Practically all the multimedia communications have been or are being placed in the network, one of the most important is the television system carried within the Internet. This system is known as IPTV. IPTV systems have experienced an unexpected success in the network, gaining in popularity compared with other television transmissions. The reason we may find in the fact that consumers, always more, "demand personalized TV experiences that are available anytime, anywhere, on any device"[2]. The capabilities of IP television to fulfill these requirements as well as the fact that the whole complexity of IPTV systems is actually transparent to the consumers give more and more popularity to IPTV systems.

IP television favored changes in business models for the Internet. While before IPTV introduction, users connected more or less occasionally, now with IPTV (classical television or video on demand) the users just do not disconnect the computers from the Internet. The result is that many more consumers are constantly connected and the classical IPv4 addressing is not enough. IPTV demands IPv6 to offer static addressing to all the users. Moreover, another reason for the introduction of IPv6 to carry IPTV streams is the mobility of terminals (UMTS, LTE, etc.). As known, mobility requires enlarged addressing. On the other hand, we may remark another not banal reason for carrying classical television channels by IPv6 network is the enhanced multicast of IPv6 compared to earlier version of Internet protocol. Therefore, IPv6 seems to be crucial for IPTV.

Japan was the first country, which implemented a complete IPTV system working on IPv6. This first system is NTT Plala Hikari TV[3] and its implementation resulted indispensable since Japan developed only-IPv6 network. In any case, Hikari TV resulted very successful and currently has hundreds of thousands of consumers. Toshiba was the first hardware-specialized company commercializing IPTV devices working on IPv6.

The complexity of IPTV systems is due to the high quantity of information carried by television streams. In fact, the IPTV is known as one of the killer applications in the Internet because of the necessity of bandwidth. The demand of higher quality of the images required by the consumers means in practice that the image resolution is always higher and it implies more bandwidth in the IPTV transmissions. Figure 1 shows different image resolution codes (most typical in Europe) standardized or commercialized in the indicated years. As we may observe, the proposed image resolution generally increased as time went by.

To this increasing image resolution, we should add the higher requirements of television 3D, which in its most popular version, consists of uniting two images in one, doubling, in this way, the necessary bandwidth in the network.

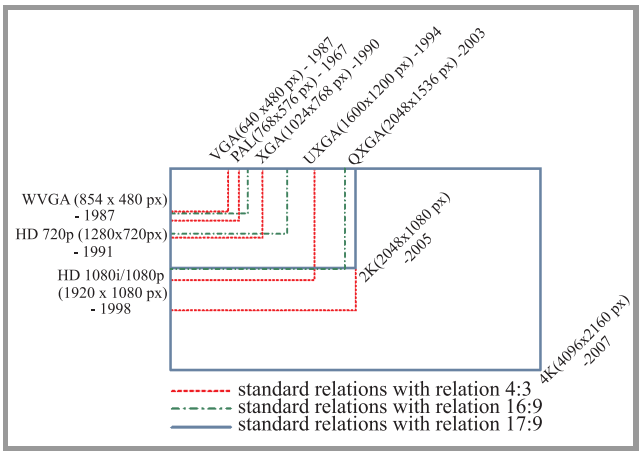


Fig. 1. Standards for image resolution.

Moreover, new applications related to the IP television as, e.g., interactive television, demand new requirements from the network. In the case of interactive television, the requirements are more similar to the interactive games than to the classical television.

For the correct management of heavy TV streams served to an increasing demand, the IPTV systems are developing and improving new solutions every day. In this sense, IP television comprises many research areas related to telecommunications. These areas are, among others, storage technologies, video and audio encoding (for example, MPEG-2 codec or more recent MPEG-4 H.264 codec), data encryption, data distribution, transmission by the network (new control and data planes). The complexity of IPTV systems as well as their importance is also proved by the increasing number of projects dedicated to improvement of transmission of television streams by the Internet. Between all the projects within the 7th Framework Program funded by the European Union (EU 7FP) we may highlight the following ones: one of the most successful projects, which is currently finishing is the P2P-Next project[4]. Among other objectives, this project specified and implemented a set top box with an interface for connecting to peer to peer networks which offers to the classical television sets the possibility of gaining access to the contents provided by peer to peer networks. Mobile3DTV[5] researches problems of moving 3D television to mobile environment. As known, mobility has strong limitations of bandwidth availability, which is not according to 3D television bandwidth requirements. Challenges as capture of 3D images, coding, and transmission are investigated in Mobile3DTV. Otherwise, CANTATA[6] is a project proposed inside the information technology for European advancement (ITEA) and develops a subset of functionalities related with interactive TV systems, which defines the requirements for this kind of television. Interactive TV enhances IPTV by offering to the consumer the possibility of interacting with the service provider for, e.g., shopping purposes. Many other

[2] www.ericsson.com/campaign/televisionary
[3] www.hikaritv.net
[4] www.p2p-next.org
[5] www.mobile3dtv.eu
[6] www.itea-cantata.org

7FP projects aim at introducing content-awareness within the network, which will undeniably open many new business possibilities to the Internet television. In fact, the new proposed architectures interconnect the four actors delineated in IPTV systems: content providers, IPTV service providers, transport and distribution IP network providers and clients [3]. These projects are grouped together in the future media networks cluster.

Let us remark that IPTV refers not only to classical broadcast television but also to new video on demand (VoD) services. The difference between them lies in broadcast (or multicast) transmission of classical television channels and unicast (or anycast for new content aware network architectures) of VoD transmissions. Anyway, the system studied in this paper refers to classical broadcast (multicast) television.

The concept of our IPTV system is presented in Fig. 2. In this system, the high definition television signal, called digital video broadcasting or briefly (DVB) can be delivered either by satellite (DVB-S) or terrestrial (DVB-T) manner. After receiving by appropriate antenna, television signal is transferred to the dreambox device. The dreambox[7] is a type of set top box and it is responsible for splitting digital DVB signal into IP packets, buffer them and transmit to the network as an integrated IP packet stream. Because unicast communication is not effective for providing IPTV service, often multicast connections are used for transfer packets between dreambox and end devices. Users can watch TV programs directly on their PC computers or laptops, thanks to appropriate IPTV applications. In case when we want to use a display unit such as a TV set, another set top box (STB) is used to transform again the IP packet stream into high definition television signal.

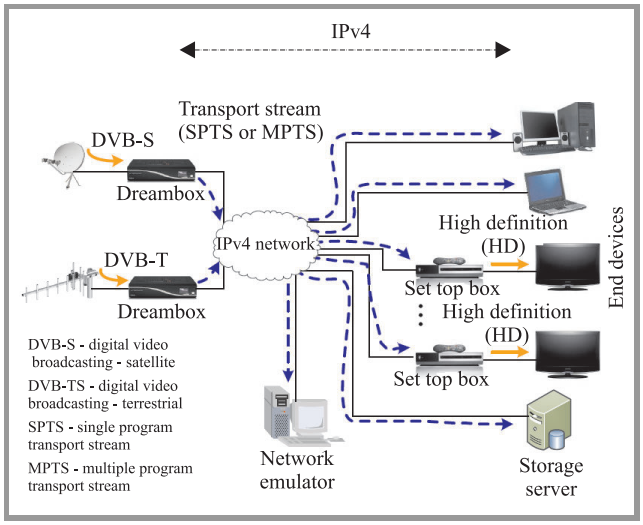


Fig. 2. IPTV system over IPv4.

The IPTV data are transferred through the network as a transport stream (TS), which is defined in MPEG-2 specification [4]. The TS is a type of container used for multiplexing the audio, video and auxiliary data as, for example, information required for synchronization or error correction. Transport stream is then packetized and encapsulated into the IP packets. MPEG-2 standard distinguishes between two types of TS: single program transport stream (SPTS) and multiple program transport stream (MPTS). SPTS correspond to transmission of a single TV channel, whereas MPTS allows transfer of more TV channels together within the same TS. The part of MPTS stream is program associated table (PAT), which contains the list of all transmitted TV channels. From the network point of view, the most important difference between the SPTS and MPTS is the necessary bandwidth for transmission. As we will see further below, this difference results crucial for the efficiency of the proposed IPTV solution for IPv4/IPv6 environment.

The stated IPTV system additionally contains a server to storage transmitted video files for further use, as well as a network emulator to perform diverse measurements in the IPTV system, such as measurements of QoS metrics experienced by IPTV flows for different (e.g., high load) network conditions.

The IPTV system described above was originally built to work on IPv4 only. Our aim was to migrate it on IPv6 protocol. The first difficulties that we met during this process were related with used IPTV application, which does not cooperate with IPv6.

Problems with applications may hinder the widespread use of IPv6 protocol. Although many applications nowadays are already IPv6-enabled (especially those associated with Linux system[8], the process of adapting some of them to support IPv6 is still pending. For example, up to year 2009, the MySQL application, a very popular open source database, makes possible the communication over IPv6 protocol between MySQL main programs (mysqld), called MySQL servers, as well as between the MySQL server and the MySQL cluster management server program (ndb_mgmd). Nonetheless, for now the communication between ndb_mgmd program and database repositories (the MySQL cluster data node daemon – ndbd program) is still IPv4-only aware [5].

In our IPTV system, we replaced the existing IPv4 commercial application by the open-source VideoLAN Client (VLC) media player [6]. VLC can handle most of the media codecs and video formats, as well as various streaming protocols. It permits also to send and receive data using both IPv4 and IPv6 protocols. Observe that using IPv6-aware application is obligatory at least in these networks, which are natively IPv6-only. VLC cooperates with video LAN manager (VLMa), which is able to manage broadcasts of TV channels from DVB-S or DVB-T sources and streaming audio and video files. Furthermore, VLMa can be used to stream a received unicast stream in multicast way.

The main problem we found during IPv4/IPv6 migration was that the set top box (STB) devices, used to convert

[7] www.dream-multimedia-tv.de/en

[8] See e.g. www.deepspace6.net/docs/ipv6_status_page_apps.htm

IP packet stream into television signal, could not operate with IPv6 protocol. This issue does not affect dreambox devices, which work on Linux-based operating system Enigma2. Enigma2, as a large majority of Linux variants, supports IPv6. Moreover, thanks to open source concept of Linux, dreambox software can be easily upgraded by users, if need be. Unfortunately, we were not able to modify software in other STB devices. Taking into account that we had many such STB devices, it was not viable to replace all of them in IPv6-compatible equipment. To solve this, we proposed to divide the network into two subdomains, isolating the devices, which may work on IPv6 and these ones, which may work on IPv4 only.

3. Transmission of IPTV Streams on IPv4/IPv6 Environment

Creating two networks, which separate the IPv4 and IPv6 equipment, effects on the MPEG-2 transport stream transferred through the network between dreamboxes and end devices. Now we should send the transport stream twice:

– in IPv4 subdomain, transport stream is encapsulated into IPv4 packets, what is done by dreamboxes,

– in IPv6 subdomain the same transport stream is encapsulated into IPv6 packets.

To perform the latter, we propose to use special tool, called the IPv4/IPv6 server. This server is placed at the border between IPv4 and IPv6 networks and has two network cards. One of them receives multicast IPv4 stream generated by dreambox, while the second one is responsible for resending the same stream after encapsulating it in multicast IPv6 packets. Figure 3 presents the concept of resulting network. Summarizing, the IPv4/IPv6 server works as a gateway between the networks.

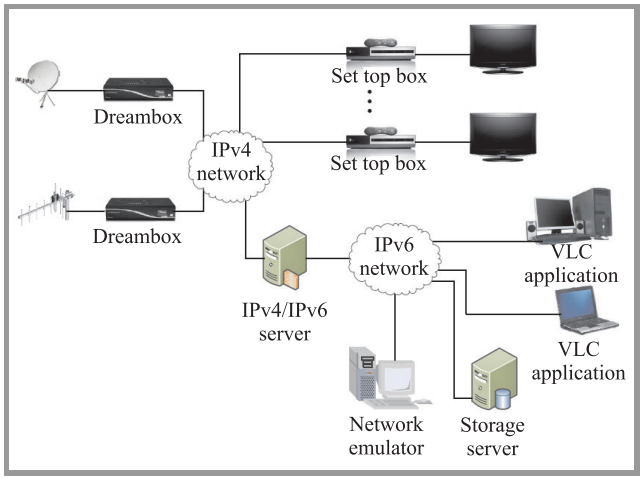


Fig. 3. IPTV system in IPv4/IPv6 environment.

In the IPv4 domain, the IPv4/IPv6 server acts as an ordinary multicast client, which subscribes to the IPv4 multicast stream in a standard way, using IGMP protocol [7]. On the other hand, in the IPv6 domain, the IPv4/IPv6 server operates as a shared root of distribution tree for an IPv6 multicast group. We assume that in the IPv6 network the protocol independent multicast – sparse-mode (PIM-SM) [8] is implemented, which is the most widely used multicast routing protocol because of its independency from underlying unicast routing protocols and overcoming the scalability problems [9]. In our case the IPv4/IPv6 server plays role of a so-called PIM-SM rendezvous point (RP) for the entire IPv6 domain. An RP can be considered as the meeting place for sources and receivers of multicast data. Setting up the IPv4/IPv6 server as a RP is crucial if there are more routers in the path between the IPv4/IPv6 server and the end IPv6 multicast clients.

RFC 3956 [10] defines an address allocation policy (called embedded-RP) in which the address of the RP is encoded in an IPv6 multicast group address. The document specifies a subrange of unicast prefix-based IPv6 multicast addresses [11], which starts with FF70::/12 prefix, by setting one of previously undefined bit from flags field to 1. Furthermore, it prescribes a method for embedding the RP address, which serves given multicast group, to IPv6 multicast address of this group. Thanks to it, there is no requirement for any multicast pre-configuration of the other routers belonging to multicast tree, if they are not operating as an RP, because routers can automatically obtain information about the RP from IPv6 multicast group address.

According to RFC under consideration, we enforce the multicast group address to be

FF77:0xxx:aaaa:aaaa:aaaa:aaaa:gggg:gggg,

where all the bits “x” together with “a” bits represent the rendezvous point address, whereas “g” bits represent the identifier of the multicast group. For implementation purpose, we notice that our IPv6 multicast group address should be mapped into Ethernet multicast address on the following form: 33:33:gg:gg:gg:gg [12].

Now we illustrate the procedure of establishing multicast connection by one IPv6 host, which wants to receive the IPTV stream generated by the IPv4 dreambox. Let us suppose, for the sake of argument, that:

– dreambox has the IPv4 address 210.165.23.7,

– the IPv4/IPv6 server has the IPv6 address
FF77:0130:1111:1111:1111:1111::,
which enclose the embedded rendezvous point address 1111:1111:1111:1111::1.

Therefore, the embedded-RP multicast prefix is

FF77:0130:1111:1111:1111:1111::/96.

To start receiving the dreambox IPTV stream, the IPv6 host should send a multicast listener report message of multicast listener discovery protocol (MLD) [13] to the destination multicast group address FF77:0130:1111:1111:1111:1111:210.165.23.7. When the IPv4/IPv6 server receives this message, it joins the new host to given IPv6 multicast group. Next, if there was no transmission of multicast data so far (since there was no

any IPv6 multicast listener), the IPv4/IPv6 server starts resending the IPTV stream to the joined IPv6 host.

Because the IPv4/IPv6 server operates in IPv6 domain as a source of IPTV streams, the IPTV packets will arrive to the IPv6 host with source address of the IPv4/IPv6 server. It means that IPv6 multicast transmission is performed with destination multicast group address FF77:0130:1111:1111:1111:1111:210.165.23.7 and source address FF77:0130:1111:1111:1111:1111::. In this way, different multicast streams from more than one dreambox are allowed if they have different IPv4 addresses. However, resending more IPTV streams by the IPv4/IPv6 server could cause incorrect work because of hardware limitations. The effectiveness of the IPv4/IPv6 server we study in the next section.

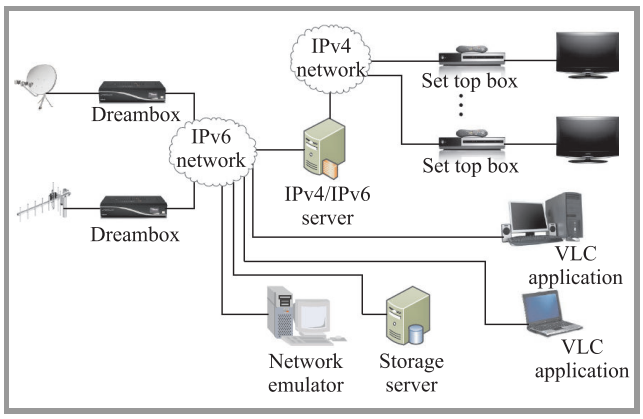


Fig. 4. IPTV system in IPv4/IPv6 environment (second approach).

The second investigated approach is when dreambox sends IPv6 stream and the server is the responsible to translate the stream into IPv4 as shown in Fig. 4.

In this case the server uses the MLD protocol to join to IPv6 multicast tree in the IPv6 network. On the other hand, in the IPv4 domain, the IPv4/IPv6 server operates as a shared root of distribution tree for an IPv4 multicast group.

4. Effectiveness Study of the Proposed Solutions

In this section we aim at investigating the effectiveness of the IPv4/IPv6 server in both the proposed solutions, i.e., when the server translates IPv4 stream into IPv6 and in the opposite way.

In the first approach, we assume that the dreambox at the IPv4 domain sends an IPTV packet stream at rate, which increases from one trial to the next. For this purpose the dreambox works in MPTS mode. The MPTS service allows to group together many TV channels, which may be encoded with standard definition (SD) or high definition (HD) resolution. During the tests, dreambox generates one MPTS flow with different number of TV channels, and then the total bandwidth of IPTV stream can be easily obtained as multiplication of bandwidth of the SPTS flow (9.47 Mbit/s). Although we could increase IPTV data rate by simply growing the number of SPTS multicast flows, we believe that the chosen approach imitates better a real IPTV scenario, where one IPTV service provider offers different number of TV channels. Then we monitor whether the IPv4/IPv6 server is able to transfer received IPTV packets to the IPv6 network.

The test run as follows: firstly the multicast tree was created in both IPv4 (using IGMP protocol) and IPv6 domains (using MLD protocol). Next dreambox streamed the DVB-T signal as a unique SPTS in IPv4 multicast mode. The IPv4/IPv6 server captured the IPTV stream as IPv4 multicast listener, and resent it to the IPv6 end devices in an IPv6 multicast connection. We calculated the rate of packet flow received by the IPv4 network card of the IPv4/IPv6 server (incoming stream) and the rate of packet flow sent by the IPv6 network card (outgoing stream). The obtained results are presented in Fig. 5.

After that, we changed SPTS for MPTS flow and repeated the tests for increasing number of TV channels encoded in the stream. Logically, when MPTS contains more channels, larger bandwidth is necessary to transfer it. In the same way as previously, we calculated the data rate of the incoming stream (to the IPv4/IPv6 server from IPv4 network) and the outgoing stream (from the IPv4/IPv6 server to the IPv6 network). Figure 5 presents these values.

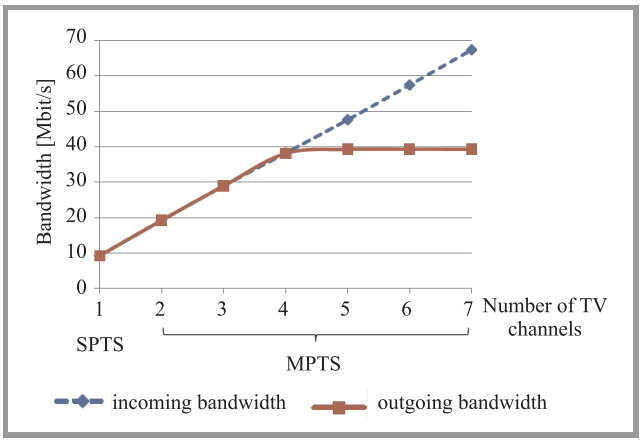


Fig. 5. Results of IPv4/IPv6 server's effectiveness (SPTS – single program transport stream, MPTS – multiple program transport stream).

As one can observe, for low rates the IPv4/IPv6 server does not affect resent IPTV stream. The limit value corresponds to four SPTS flows' bandwidth. Higher rates of IPTV traffic results in packet losses within the IPv4/IPv6 server. We may indicate that the hardware limitations of the server cause this effect. The IPv4/IPv6 server was implemented on PC with processor Intel® Core™2 duo desktop processor E8500 3.16 GHz and Linux operating system with kernel version 2.2.17. Anyway, presented studies show that the proposed solution has limitations. Certainly, the IPv4/IPv6 server may be used for providing to user a single TV channel (SPTS) as, e.g., a football match in a pay-per-view video service, but the hardware limitations cause that it is not

suitable for serving, e.g., the public television, which transmits many TV channels.
In the second approach, we assume that IPTV packet stream is sending by the dreambox, which is in this case located in the IPv6 domain. As in the previous test, the dreambox generated IPv6 packets with increasing rate by working in MPTS mode and emitting the same number of channels as described above. The hardware used to implement the IPv4/IPv6 server was the same one.
The test run similarly to the preceding one, i.e.: firstly, the multicast tree was created in both IPv6 (using MLD protocol) and IPv4 domains (using IGMP protocol). Next dreambox streamed the DVB-T signal as SPTS or MPTS (in consecutive trials) in IPv6 multicast mode. The IPv4/IPv6 server captured the IPTV stream as IPv6 multicast listener, and resent it to the IPv4 set top boxes in an IPv4 multicast connection. We calculated the rate of packet flow received by the IPv6 network card of the IPv4/IPv6 server (incoming stream) and the rate of packet flow sent by the IPv4 network card (outgoing stream). The obtained results are presented in Fig. 6.

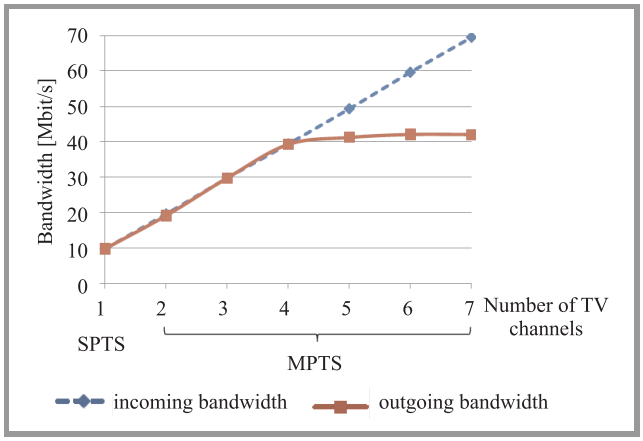


Fig. 6. Results of IPv4/IPv6 server's effectiveness (SPTS – single program transport stream, MPTS – multiple program transport stream) – second approach.

As we may observe in Fig. 5 and Fig. 6, the effectiveness is very similar in both of the approaches. The minimal differences (rather imperceptible in the figures) in favor of the second option could be provoked by the more complexity in sending multicast IPv6 packets than multicast IPv4 packets.

5. Conclusions

To support smooth transition between IPv4 and IPv6 protocols, a set of *good practices* in this direction should be proposed. In this paper we present a solution for deploying the IPTV system in an scenario which involves presence of two kinds of devices: IPv4-only and IPv6-only. The proposal exploits special server for transferring IPTV multicast traffic among IPv4 and IPv6 domains. The proposed solution may be framed as one of these *good practices* because it allows a simple step towards widespread introduction of IPv6.

From the performed experiments we could demonstrate that our IPTV system properly works on IPv4/IPv6 environment. As a consequence, we may conclude that the presented implementation issues are correct. We implemented two solutions, the first one when the multicast IPv4 stream is translated into multicast IPv6 stream and the second one in the opposite direction. Both the solutions properly worked and showed that they may be valid solutions for the case when IPv4-only and IPv6-only receivers are in the IPTV system.
On the other hand, the obtained results of effectiveness let us to realize that, in case of large bandwidths of IPTV streams, the proposed IPv4/IPv6 server does not properly run and is not capable to transfer the whole incoming IPTV traffic. We deliberated that this issue depends on the used hardware but it should be an advice note when one considers using the proposed solution in systems, which demand high bandwidth as classical IPTV does. The effectiveness of the two proposed solutions is similar and it is not possible to conclude which of them behaves better in wide IPTV systems.

References

[1] "Mu Dynamics introduces Mu Test Suite for IPv6 to significantly accelerate and ensure successful IPv6 migration", Mu Dynamics Inc. 2010 [Online]. Available: http://www.tmcnet.com/usubmit/2010/04/26/4749761.htm
[2] C. D. Marsan, "YouTube turns on IPv6 Support, net traffic spikes", *PCWorld Mag.*, Feb. 2010.
[3] D. H. Ramirez, *IPTV Security: Protecting High-Value Digital Contents*. Wiley, 2008.
[4] "Information Technology – Generic Coding of Moving Pictures and Associated Audio Information: Systems", ITU-T Recommendation H.222.0, Inst. Telecommun. Union, Geneva, Switzerland, 2000.
[5] *MySQL 5.1 Reference Manual*, paragraph 17.7.2.22. Oracle USA, January 2009.
[6] "VLC media player: The cross-platform open-source multimedia framework, player and server" [Online]. Available: http://www.videolan.org/vlc/
[7] B. Cain, S. Deering, I. Kouvelas, B. Fenner and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, IETF, October 2002.
[8] B. Fenner , M. Handley, H. Holbrook, I. Kouvelas, "Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)", RFC 4601, IETF, August 2006.
[9] E.-M. Lee, Y.-T. Han, H.-S. Park, "Rendezvous point relocation for IPTV services with PIM-SM", in *Proc. 14th Asia-Pacific Conf. Commun. APCC 2008*, Tokyo, Japan, 2008.
[10] P. Savola and B. Haberman, "Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address", RFC 3956, IETF, November 2004.
[11] B. Haberman and D. Thaler, "Unicast-Prefix-based IPv6 Multicast Addresses", RFC 4601, IETF, August 2002.
[12] M. Crawford, "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, IETF, December 1998.
[13] R. Vida and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, IETF, June 2004.

Jordi Mongay Batalla – for biography, see this issue, p. 11.

Piotr Krawiec – for biography, see this issue, p. 13.

Paper

On Testing IPv6 in Small ISP's Networks

Konrad Sienkiewicz[a], Mariusz Gajewski[a], and Jordi Mongay Batalla[b]

[a] National Institute of Telecommunications, Warsaw, Poland
[b] Warsaw University of Technology, Warsaw, Poland

Abstract—Testing process allows to detect potential faults of implementation of IPv6 in the phase preceding migration, thus minimizing the risk of problems in IPv6 deployment. In general the IPv6 tests should be performed by all network providers, however the test range should fit their needs. It causes that test range for small network operators (offering basic set of services) could be limited in comparison to larger ISPs. In this paper, we propose an approach to IPv6 tests with regard to IPv6 deployment by small operators. We present tools and specifications for IPv6 tests and propose a test platform optimized to small ISP's needs. The test platform is a dedicated LiveCD distribution based on FreeBSD operating system with IPv6 test environment and set of pre-defined tests. An advantage of this solution is the ability to launch the test tool software on any computer equipped with an Ethernet card and CD-ROM/DVD-ROM drive. LiveCD test tool allows users to execute tests and analyze the results in graphical environment.We believe that this approach will help to simplify and shorten the IPv6 testing process in small ISP's networks.

Keywords—conformance testing, interoperability testing, IPv6.

1. Introduction

Many efforts were submitted by the standardization organizations to define tests necessary to validate IPv6 implementations. The most famous standardization organization on IPv6 is the IPv6 Forum[1], which launched the IPv6 Enabled Logo program. The goal of the so-called Logo programs is to accelerate the deployment of IPv6 by specifying the necessary tests and offering the testing tools for conformance tests as well as for interoperability tests. Furthermore, many projects in Europe, US, Japan, China and elsewhere were directed to implement the tools for the defined tests. Enormous amount of tests suggests these don't suit needs of small operators, who need test solutions meeting the following requirements:

- Simplicity: easy to use, limited number of test cases (as needed), based on Unix-like OS.
- Low cost: use of free software and possibility to launch using PC.

Moreover from the point of view of the areas, where IPv6 is implemented and where not, we notice that small ISPs (small operators) have limited human and hardware resources, and possibly lack knowledge about migration to IPv6. On other hand, big network operators as well as service and content providers seem to be able to introduce IPv6 by themselves.

These are reasons why we focus in this paper on needs of small operators with regard to IPv6 testing aspects. We think that offering a selection of tests according to the needs of small providers and preparing a freeware test platform to be published before long may be very useful for deployment of IPv6 in small networks.

In the next section, we present basic tests associated with ISP needs and current IPv6 test tools, distinguishing between commercial and open-source software. Afterwards, we focus on open-source test tools being the best for IPv6 deployment in small domains. Section 4 presents the selection of tests considered strategic for small providers.

2. Principles of Testing

The IT industry performs IPv6 tests to satisfy requirements, which are different in case of equipment suppliers and providers. The equipment suppliers mainly focus on conformity to IPv6 standards whereas the providers rather focus on assurance of efficient interworking with other IPv6 equipment within the network. Generally, tests of network hardware cover three fields: conformance, interoperability and performance. These test types are shortly characterized below. **Conformance tests** are performed to determine whether a particular piece of equipment satisfies the specified criteria of operation. Conformance testing methodology defines the boundaries of the system under test (SUT) as well as the test system responsible for monitoring the SUT behavior. Because the test system controls the sequence and contents of the protocol messages sent to the SUT, it can impose a wide range of both expected and unexpected (invalid) behaviors. Thus, test system can emulate all network nodes which communicate with SUT. To sum up, conformance tests check whether given implementation conforms to protocol specification.

The purpose of **interoperability tests** (also called "Network Integration Testing" according to ETSI TR 101 667 [1]) is to prove the functionality between, at least, two communication systems situated in operating environment. The testing system comprises one or more devices (so called reference hosts or reference routers) from

[1] www.ipv6forum.org/

Table 1
Comparison between conformance testing and network integration testing [1]

	Conformance testing	Network integration testing
Goals	To verify that a protocol implementation conforms to the relevant protocol and profile specifications, ⇒ CONFORMANCE	To verify that a complex network is able to provide user with services in a correct, homogeneous and reliable way, ⇒ SERVICE, FUNCTIONALITY
Object	The implementation of an OSI protocol specification in a network element	A network, or part of it, made up by joining two or more network elements
Process phases	1) specification of an ATS, ICS and IXIT 2) realization of means of testing 3) conformance assessment process (or second party testing)	1) specification of an ATS, ICS and IXIT 2) agreement between different network operators 3) realization of independent means of testing (one for each test laboratory) and of the TCPs 4) result collection
Type of test	Local or dual 1) basic interconnection tests 2) capability tests 3) valid behavior tests 4) inopportune behavior tests 5) invalid behavior tests	Dual only 1) basic interconnection tests 2) valid behavior tests 3) connectivity tests 4) stability and performance tests
Users of the methodology	Manufacturers (to guarantee that their products conform the national and international protocol and profile specification) and network operators (for the same reason)	Network operators (for guarantee their customers that the network is able to provide the subscribed services in a correct and reliable way)

different vendors besides the equipment under test. The equipment under test and the reference equipment together define the boundaries of the interoperability test. In opposite of conformance testing, interoperability tests are performed on interfaces that provide normal user control and observation (no network nodes emulation). Interoperability tests are based on functionality accessed by the user.
These tests are related to normal interworking and do not contain inopportune behavior and invalid behavior tests and therefore, the list of interoperability test cases is shorter than during conformance tests. It could potentially decrease test execution time. On the other hand, interoperability tests should be performed in real environment; they require to more hardware and time compared to conformance testing in order to prepare the test configuration.

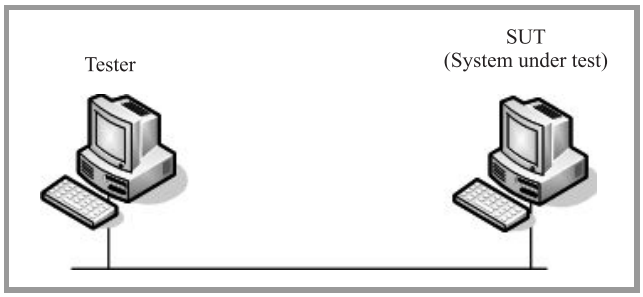


Fig. 1. Sample block diagram for conformance test environment.

Note that devices should be manually configured. Figure 1 presents two exemplary test configurations, one for conformance and the other one for interoperability test, whereas Table 1 presents general differences between both the types of tests.

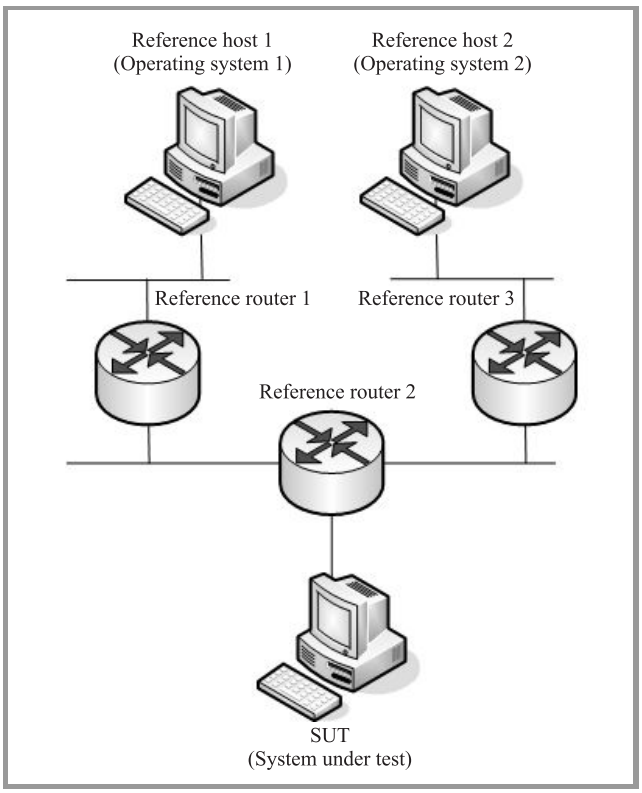


Fig. 2. Sample block diagram for interoperability test environment.

Network operators often need a close working relationship with vendors to solve unforeseen problems, e.g., interface incompatibilities, which may even imply hardware reconfiguration and software tuning. The result is often a delayed introduction of services, which implies a negative impact on the brand, with increased costs due to necessity to handle customer's complaints. Software upgrades and new version releases also pose notable challenges for operators, who should ensure interoperability within existing networks based on different system vendors and architectures. As a result, interoperability testing of new network technologies with legacy systems became highly costly and time consuming. Moreover, the pressure on operators increased due to shorter and shorter time-to-market of new services required. Consequently, it is particularly important for providers (especially small ISPs) to use a specific, cost-effective, overall testing methodology, assuring an optimal time-to-market for each new service to be deployed; this is specially accentuated when introducing IPv6, because almost all the network hardware must be tested.

Apart from interoperability testing, small ISPs are also interested in **performance tests**, which determine effectiveness of data transmission in their networks. However this group of tests is out of scope of this paper because performance tests depend on the specific services and specific network functionality.

3. Test Specifications and Platforms

This section includes the state of the art of projects focused on IPv6 testing. Especially we describe works on specification of IPv6 tests as well as currently available test platforms delivered by commercial suppliers and non-profit projects.

3.1. Test Specifications

Basically two standardization organizations have the leading position for IPv6 testing; they are IPv6 Forum and ETSI.

The IPv6 Forum is a world-wide consortium focused on providing technical guidance for the deployment of IPv6. To IPv6 Forum belongs the IPv6 Ready Logo Committee, whose mission is to define the test specifications for IPv6 conformance and interoperability testing, to provide access to self-test tools. Devices that passed all the tests can be marked with the IPv6 Ready Logo.

ETSI established the Specialist Task Force 276 (STF276) which worked on IPv6 testing. ETSI STF276 project has provided a publicly available test development framework as well as interoperability test packages for four key areas of IPv6: core protocol, security, mobility and transition from IPv4 to IPv6. The approach is based on flexibility and extensibility to facilitate testing of IPv6 products for interoperability in many contexts including development, procurement and certification schemes. The work were done in a close relationship the IPv6 Ready program of the IPv6 Forum. The project objectives were to:

- produce publicly available (standardized) IPv6 interoperability test specifications,
- reduce the cost of testing and test development through the standardization of an IPv6 test development framework and TTCN-3 library,
- contribute to the implementation of the eEurope 2005 Action Plan,
- strengthen the European influence in the IPv6 Ready certification program,
- actively support and involve stakeholders in the standardization of IPv6 test specifications and the IPv6 certification process,
- contribute to the rollout of reliable and interoperable IPv6 network products.

Besides IPv6 Forum and ETSI specifications, there are test specifications developed by test tool vendors too. These test suites are related to their (commercial) testing solutions.

3.2. Test Platforms

Among the tools used for testing IPv6 commercial tools are available as well as free tools developed under different projects. Examples of commercial tools are:

- Test Center from Spirent,
- IxN2X from Ixia,
- diversifEye from Shenick.

Each of above solutions consists of hardware platform and test suite supplied by the manufacturer. The choice of commercial tools have provide a number of advantages (e.g., like performance, and customer support), but a relatively high price is a disadvantage of these solutions. It should be assumed that for many small operators buying such a tool is unprofitable. Therefore they should focus on available free available test tools which are developed under different projects. Among them we recommend paying attention to TAHI [2] and Go4IT [3] projects, both these projects are popular among researchers, what provesing the correctness of the choice (i.e., [4]–[6]).

The TAHI project was launched in 1998, its main goals are support of IPv6 deployment by providing test tool and developing test suite consisting of conformance and interoperability tests. The TAHI Conformance Test Suite is a bundle of software based on FreeBSD, consisting of a conformance test tool and a conformance tests packages dedicated to different functionalities of IPv6. Conformance test tool consists of two parts: V6eval and KOI. V6eval is designed to develop tests for IP layer protocol test and KOI is designed to develop tests for application layer protocol test, using sockets API of operating system it works on. V6eval

presumes a test environment with a tester node (TN) directly connected to the system under test (SUT) via one or multiple Ethernet interfaces, depending on SUT type. This environment is shown in Figs. 3 and 4.

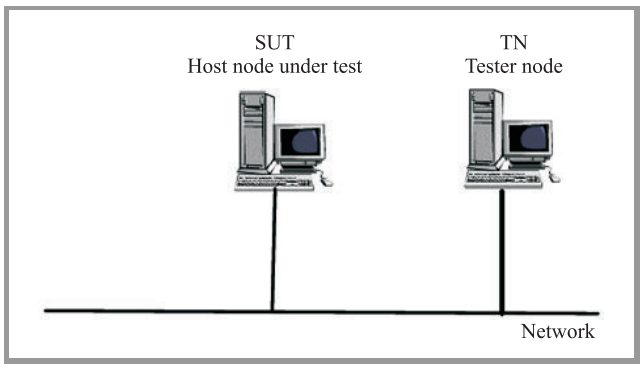


Fig. 3. TAHI test environment for host.

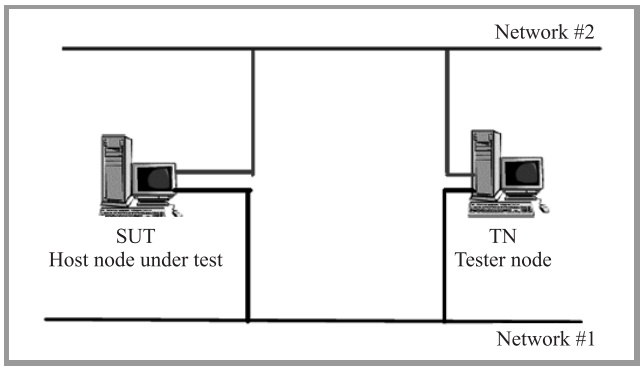


Fig. 4. TAHI test environment for router.

In order to fully automate the testing process, an RS-232 connection should be arranged between the TN and the SUT, over which commands can be sent from the TN interactively. V6eval supports remote control scripts for more than 30 different IPv6 implementations in order to automate the testing process. Currently, TAHI test suites cover the following areas:

- IPv6 Core Protocols including
  - IPv6 Specification (RFC2460),
  - ICMPv6 for IPv6 Specification,
  - Neighbor Discovery for IP Version 6 (IPv6),
  - IPv6 Stateless Address Autoconfiguration,
  - Path MTU Discovery for IP version 6,
  - Transition mechanisms for IPv6 hosts and routers (IPv6 over IPv4 tunnel),
  - Default address selection for IPv6,
  - NAT-PT,
- IPSec (v6 and v4),
- Mobility Support in IPv6,
- DNS Discovery,
- Multicast Listener Discovery for IPv6,
- SIP (IPv6).

The Go4IT project was launched in November 2005 and aimed to provide a TTCN-3-based test environment for IPv6 protocol testing including related test tools, test suites and associated testing services. The motivation for the development of this test tool has been the lack of freely available test execution environment for IPv6 testing based on TTCN-3. The TTCN-3 testcases are defined in ETSI STF 276. The Go4IT project has gone in two directions, leading to development of package 1 and package 2. Package 1 is focused on creation of downloadable, easy and ready to use executable TTCN-3 test suites for IPv6 protocols. Package 2 is focused on the development of an open TTCN-3 test development environment that allows users to develop and execute their own test cases. To fulfill the objectives defined for Package 1, a test tool, named "Go4IT IPv6 executable test suites" (GIPETS) including ready to use executable IPv6 test cases, has been developed.
Release 2.0.0 of GIPETS includes 497 IPv6 ready to execute test cases for IPv6 Core protocol, IPsec and IPv6 Mobility.

4. Test Platform Recommended for Small ISP

To meet the expectations of small operators we propose new approach in IPv6 area. Currently we are working on deployment of a dedicated test tool for IPv6 testing in their networks. This tool is based on the TAHI platform. An advantage of this solution is the ability to launch the test tool software on any computer equipped with an Ethernet card and CD-ROM/DVD-ROM drive. Using this test tool does not require FreeBSD and the TAHI environment installation, which greatly accelerates and simplifies the preparation for the tests. This is achieved through the preparation of a dedicated distribution LiveCD based on FreeBSD operating system including TAHI environment and selected test suite. A Live CD distribution is an entire operating system that is contained on a removable medium such as a CD or DVD. Because the entire operating system is on the CD or DVD, and uses PC RAM to hold temporary data, the user can run the test tool without touching the contents of hard disk. It's important that all software packages included in LiveCD do not require installation.
Another distinguishing feature of this distribution is test suite, tailored to small operator needs. The main purpose of these tests is to check functionality usually verified within interoperability tests These are tests executed in a simply configuration used for conformance testing. Mentioned above FreeBSD distribution with test environment and set of pre-selected tests is currently under work. At the moment we have already developed pre-release version of LiveCD tool which allows users to execute tests and an-

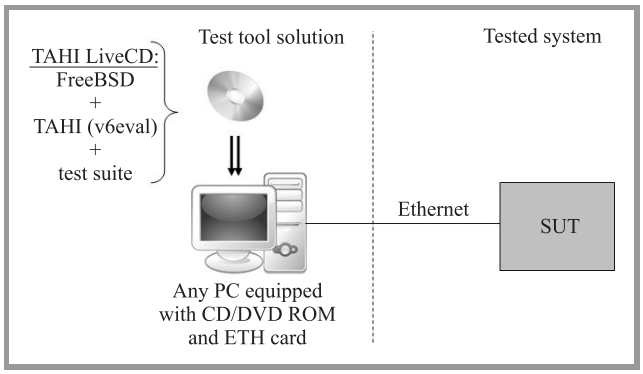


Fig. 5. Proposed solution based on TAHI LiveCD distribution and selected test suite.

alyze the results in graphical environment. The LiveCD tool includes following main software packages:

- FreeBSD 8.0,
- V6eval v3.0.1,
- Wireshark v1.2.2,
- Perl 5.8,
- XFCE4 windows manager,
- Lighttpd server,
- Opera web browser.

LiveCD tool contains two sets of IPv6 testcases. One of these sets is a replication of TAHI testcases. The other one is the set of selected tests optimized to small ISP needs. The set of selected tests comprise a subset of conformance tests available in TAHI project for base IPv6 functionality which is mandatory from small operator point of view. The following assumptions have been made to choose tests:

- Tests should cover functionalities commonly used by small ISPs.
- Tests should focus on mandatory IPv6 protocol features.
- Tests should cover functionality usually verified during interoperability tests.
- Chosen tests does not include tests related to handling of unexpected events which occur rarely during messages exchange.

Taking into account the above assumptions we are working on preparing a adequate testcases in following areas:

1. IPv6 Base Specification

   Tests selected in this group will address and verify that:

   – a node properly processes and generates the following fields in the IPv6 header: version, traffic class, flow label, payload length, next header, and hop limit;

   – a node properly processes and generates the following fields in the IPv6 header: the header extension length field in extension headers, and the option type and option data length;

   – a node properly times out fragment reassembly, abandons reassembly on packets that exceed a maximum size, processes stub fragments, and reassembles overlapping fragments.

2. ICMPv6 tests included in this group will verify conformance of the Internet control message protocol to IPv6 specification.
3. IPv6 Neighbor Discovery

   Tests in this group verify:

   – conformance of the address resolution and neighbor unreachability detection functions with the neighbor discovery specification,

   – that host properly performs router and prefix discover.

4. IPv6 Stateless Address Autoconfiguration

   Selected tests in this group will verify:

   – conformance of the address autoconfiguration and duplicate address detection to IPv6 Stateless Address Autoconfiguration Specification,

   – conformance of creating global addresses, processing Router Advertisements and expiring an address to IPv6 Stateless Address Autoconfiguration Specification.

5. DHCPv6 basic tests

   Tests in this group will verify correctness of server and user side implementation.

Test cases are divided in subsets by the functionality tested. Unlike TAHI environment (command-line based), LiveCD

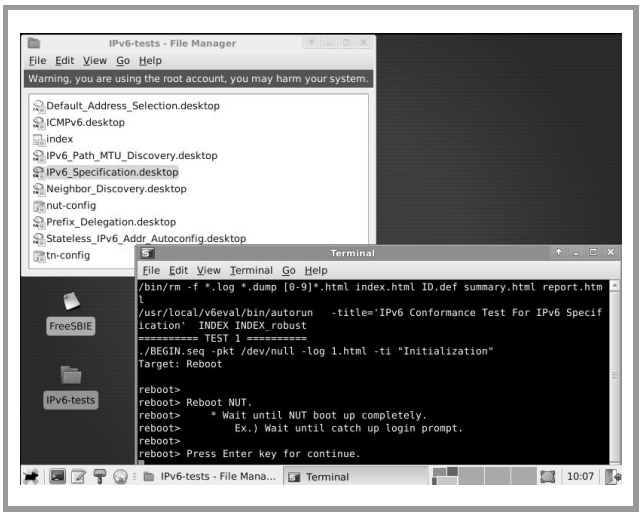


Fig. 6. LiveCD test tool – users view at the stage of selection and execution of IPv6 test.

test tool uses window-based interface (XFCE4). We believe that is a more user-friendly solution. In particular, the user not familiar with FreeBSD OS is able to configure test environment and execute the tests. To run the tests user operates on two windows. The first one is directory window where he can configure interfaces and execute subsets of tests as well as open test results in web browser. Moreover, test execution is observed in terminal window. This allows to trace test progress and respond to commands appearing during the test execution. Figure 4 shows screen during selection and execution of IPv6 test.
User can view test report in a web browser window. It contains test results as well as links to: test description, sent/expected packet description and saved packet flow as pcap file. Saved packet flow can be analyzed using Wireshark, protocol sniffer included in LiveCD tool.

5. Summary

In this paper we have briefly described the IPv6 testing process in small ISP networks and proposed an approach to IPv6 testing using a platform in a LiveCD form, which allows users to execute tests and analyze results in graphical environment. In our opinion, this approach to testing IPv6 technology in a small operator network brings several benefits. Among them, the most important are: ease of test execution - only one PC involved in testing process, reduced number of tests, test automation and finally shorter testing time. Moreover, we expect that approach based on LiveCD could be applicable to other areas. For example, we are going to use this test method in our current research project, because we want to achieve repeatability and comparability of tests performed by different teams.
As mentioned, we already have developed pre-release version of LiveCD test tool. Current work focuses on developing complete sets of tests. Final distribution will be available after completion of work from the website of Future Internet project (www.iip.net.pl).

References

[1] Methods for Testing and Specification (MTS), Network Integration Testing (NIT); Interconnection; Reasons and Goals for a Global Service Testing Approach, ETSI TR 101 667.

[2] TAHI Project [Online]. Available: www.tahi.org/

[3] Go4IT Project [Online]. Available: www.go4-it.eu/

[4] J. Ruiz, A. Vallejo, J. Abella, "IPv6 conformance and interoperability testing", in *Proc. 10th IEEE Symp. Comput. Communi. ISCC 2005*, La Manga der Mar Menor, Cartagena, Spain, 2005.

[5] Z. Jing, X. Jiang, "Protocol conformance test suite for home agent of mobile IPv6", in *Proc. Int. Conf. Elec. Commerce Busin. Intellig.*, Washington, USA, 2009, pp. 41–44.

[6] J. Lee and H. Jun Kim, "Implementation of prefix delegation mechanism using DHCPv6 protocol", in *Proc. 4th Ann. ACIS Int. Conf. Comput. Inform. Sci. ICIS'05*, Jeju Island, South Korea, 2005.

[7] ETSI IPv6 Testing [Online]. Available: www.ipt.etsi.org/

Konrad Sienkiewicz – for biography, see this issue, p. 14.

Mariusz Gajewski – for biography, see this issue, p. 12.

Jordi Mongay Batalla – for biography, see this issue, p. 11.

Paper

Dynamic Contracting of IP Services – System Architecture and Prototype

Piotr Arabas and Mariusz Kamola

Warsaw University of Technology, Institute of Control and Coputation Engineering, Warsaw, Poland
Research Academic Computer Network, Warsaw, Poland

Abstract—Proposition of architecture and implementation of prototype system for dynamic contracting IP services is presented. The system serves requests issued by users demanding setting up network service of specified parameters. DiffServ technology together with traffic engineering and admission control are used. Implementation details and results of tests are described. Necessary extensions and possibility of commercialization of such a system are discussed.

Keywords—DiffServ, dynamic contracts, IP network, quality of service.

1. Introduction

The growing demand for bandwidth is unquestioned. It results mainly from popularity of equipment allowing capture of high quality video, voice and still pictures as well as software assisting in editing and further distribution of such data. Potential users may be individuals using it mainly for entertainment (VoD, interactive games, etc.) but also companies and institutions applying them for teleconferences, distant learning or telemedicine. As such services seem to be more involving resources than others, it is natural to model influence of users' requests on them. This leads to proposition of a system for bandwidth reservation that can use information like requested start time and QoS requirements for a service to fulfill, if possible, user demands. The paper presents the project of a single domain system, as well as working prototype of limited functionality, and results of experiments.

In the last years many research projects dealt with the problem of providing QoS in IP networks, mostly assuming the existence of some signaling scheme, like the one presented in [1]. Some of them focused mainly on technical aspects, the most interesting being TEQUILA, MESCAL, AQUILA and EuQOS. In short all of them tried to build additional control layer allowing providing QoS guarantees to end users with the help of DiffServ and various methods of traffic engineering depending if they were to operate in a single (MESCAL, AQUILA) [2] or multiple domains [3], [4]. Common for all projects was an admission control logic, which seems to be necessary when providing QoS guarantees using limited resources, and poses important challenge if it is to be working in efficient, scalable way. Another stream of work was dedicated to economics of such systems, with M3I, QOSIPS and CoCOMBINE being probably the most representative projects [5], [6]. Abovementioned projects were EU-funded and had purely academic flavour. On the commercial side there are industrial standards like MPLS, DiffServ, various blends of RSVP and other reservation, monitoring and policy enforcement (e.g., SNMP, COPS, Diameter) related protocols. There is, however, no complete solution for bandwidth reservation, traffic engineering, network management and business processes; ITU NGN framework being too general and usually implemented in fragments. On the other hand vendors of network equipment offer, often expensive, software for management of their devices covering not only monitoring and maintenance but also network planning and optimization – Cisco IP Solution Center being one of examples [7].

2. Functionality and Architecture of the System

Network operators have not adopted any of the previously mentioned products and standards to build IP-based reservation systems as most of the research projects resulted only in general conception of the architecture or a limited prototype for demonstration in the laboratory. Commercial platforms, being more mature and suitable for real world application are costly, also because they must be tailored to customer needs, and maintained afterwards. All that brought the authors to the idea of developing at NASK a prototype of a reservation system – firstly, for research purposes, but with following commercial application on mind. The main function of the system is the ability to contract network resources of specified parameters: duration, source and destination points, QoS and price. The architecture is centralized as reservations are made in a domain possessed by single operator, however the inter-working is not precluded if other domains will use similar systems. Hierarchical organization is envisaged to provide scalability.

Main functional blocks and modules of the system are depicted in Fig. 1. The central element of the system is negotiations block containing logic for interaction with users and wholesale operators (needed when connection traverses

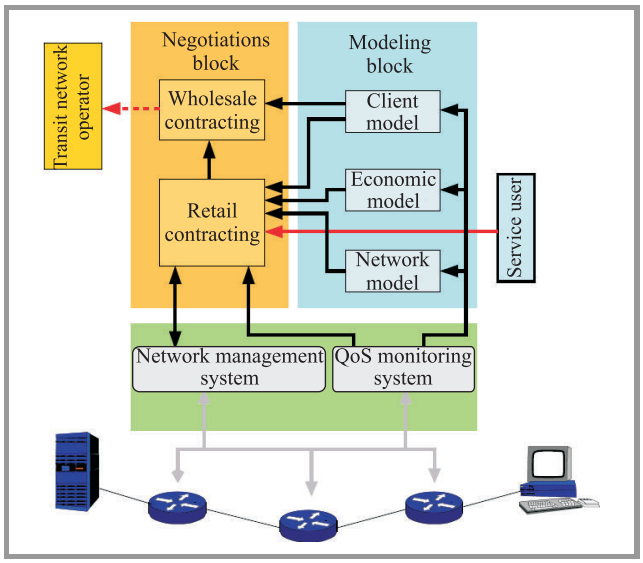


Fig. 1. Architecture of the network reservation system.

other domains). Modeling block and monitoring and actuation block serve negotiations block with necessary data and allow execution of the contract.

2.1. Negotiations Block

Negotiations block is the only block that interacts directly with users accepting or rejecting their requests. The decision whether to serve or deny a request depends on two factors:

– technical possibility of providing the service,

– profitability of the contract.

The technical possibility of providing the service is determined by the network state at the moment of the execution of the contract. As the service is usually requested in advance, technical possibilities must be predicted, taking into account:

– available network resources,

– contracts requested concurrently.

These two factors are managed by network and customer models being part of the modeling block. The first task does not pose great problem as network infrastructure is varying slowly so it is possible to tune successfully appropriate models. The other requires predicting both parameters of contracts and their utilization by users, which is much more complicated.

The definition of profitability takes into account not only simple calculation of costs and income, but also reflects long-term strategy of the provider. For example, policy of increasing margin as the network load grows will favour clients willing to pay more, and make less wealthy ones request contracts early. Acting differently, the latter ones loose chance of getting any bandwidth at a desired time. In general, policy of satisfying user requests strictly (in sense of contracts timing) is contrary to network operation economy, where costs are independent on usage, and where constant and stable utilization would fit the providers best. Combining the "maximize income" and "minimize costs" goals into a consistent and competitive pricing scheme is a demanding task.

Estimation of profitability becomes even more complicated when operator has possibility to dynamically make wholesale contracts for transit links. In such situation network resources of the operator are not constant as they may be periodically renegotiated. Such renegotiation is triggered by analysis of scheduled contracts but, reciprocally, strategy of contracting depends on transit costs. Cross dependency may be solved by assumption that wholesale contracts are valid for time longer than decision horizon of retail contracting. So, the module responsible for retail contracts may treat wholesale contracts as given and make decisions using only the economic model. Module responsible for wholesale contracts analyzes retail contracts (both accepted and rejected) ex post and, if improvement is possible, renegotiates them with wholesale bandwidth providers. This way two levels of contracting are decoupled securing global scalability of the system.

2.2. Modeling Block

Modeling block consists of three specialized models: network model, economical model and customer model. Using these models it is possible to feed negotiation algorithms with predictions necessary for computing optimal contracting strategies. Network and customer models are adjusted using traffic and contract data available in abundance from network monitoring and customer relationship management (CRM) systems. Economic model is more static due to its expert character. The task of network model is assessing network state while some set of contracts is active. A single contract C_i may be described by the following set of parameters:

– requested start and termination time – α_i and ω_i,

– requested source and destination points – o_i and t_i,

– requested average and peak bandwidth – b_i and p_i,

– requested maximum delay d_i, and its variance j_i,

– requested loss rate r_i,

– a vector of parameters $\mathbf{f}$ describing actual way of utilizing the contract by the user; it may contain parameters like the ones above, but also more specific ones w.r.t. traffic engineering: e.g., effective bandwidth [8].

Network model predicts how to configure network equipment to provide contracts in optimal way. The output of the model are variables describing working conditions of all links as well as prediction of quality parameters for contracts being available bandwidth, delay with variation, loss rate and path selected for transmitting data.

Network model refers to network topology and technology (including QoS provisioning technology) to predict utilization of resources and so state of the network. These data combined with set of contracts selected for execution constitute optimization task where the network topology, contracts and traffic multiplexing rules are the constraints. The method of providing contracts (depending on the technology of the network) defines constraints but also the performance index, e.g., when using DiffServ the contracting strategy imposes class of service but also requires to manage resources – select appropriate paths, balance loads on links etc.

The way of modeling interactions between transmitted streams depends on nature and number of these streams. One of most advanced approaches may be effective bandwidth theory [8], however it requires detailed knowledge of traffic characteristics and is applicable only in case of large number of concurrent streams. In smaller scale simplified models (mainly pessimistic) or even network simulators (e.g., ns-2 [9]) may be used. Time necessary for completing simulation precludes its on-line use, however it could be helpful for periodic tasks as traffic engineering and optimization of contracts parameters. The main reason for modeling the network is admission control – in such case a list of active contracts with paths selected for them is an additional constraint for the optimization task.

Client model predicts real user traffic pattern versus the resource consumption as declared by a user. It is fed with abundant historical traffic data. This way traffic engineering may be more effective as its input is closer to reality. It is important, however, to remember that degree of utilization of requested bandwidth is not constant. It usually depends on kind of service and it may also vary with price of service as willingness to pay may reflect meticulousness of users. This results in coupling between pricing and client modeling making optimization task more complex. The handling of such phenomenon is to use pessimistic approach for accepting contracts and tune the approximation when statistics become available.

Economic model provides relation between quantities describing services, costs and incomes generated. Association between costs and services is not straight as some costs are generated directly while others inflicted by sub-services used.[1] Fair distribution of costs should prevent unjustified lowering price of some services (while other subvent them) and so protect competition. In practice, however prices usually do not result from costs, but models of costs distribution are used internally in the enterprise to assess profitability and, when optimizing pricing strategy, become part of performance index or constraints.

As stated before, services may be provided with use of resources bought in wholesale contracts from higher tier providers. The fluctuation of wholesale prices may influence costs of services, however it is assumed that their time scale is much longer than horizon of operational decision making which thus may be performed for static set of wholesale contracts.

Economic model describes also dependency between demand for services and their prices, which may be done with well known parametric models like Cobb-Douglas model that uses elasticity to connect changes in price with varying demand or utilization [11]. Thanks to abundance of data available for dynamically contracted service model parameters may be regularly updated, preferably for models prepared separately for various market segments. Initial values of parameters must be, however, chosen when data are scarce: then expert models are to be used.

The output of economic model is used in negotiations block supporting process of wholesale and retail contracting by determining performance index. It must be stated that performance index may reflect various short term targets like maximizing volume of contracts, minimizing number of rejected requests or contracts violating QoS guarantees (to maximize number of satisfied users), but always in longer horizon it supports the same economical targets.

2.3. Monitoring and Actuating Block

Monitoring and actuating block constitutes adaptation layer between modeling and negotiations blocks and network equipment. The QoS technology is fundamental for contract providing, it must however be implemented in network equipment, and to manage equipment of various vendors uniformly, the set of communication procedures is necessary. For the same reason this layer consists of specialised procedures for monitoring state of equipment and QoS level of contracts.

Network management subsystem provides means for setting contracts, which, for DiffServ and MPLS technology, requires setting of:

- flow classification,
- traffic profiling and shaping,
- prioritizing traffic via class queues,
- MPLS queues.

Communication with network equipment may be implemented with standardized protocols like SNMP and LDAP or using telnet and CLI. The efficiency and complexity of both approaches is similar, the main problem being laborious checking of correctness of configuration.

[1] Establishing a fair cost-splitting scheme for common networking infrastructure is a task of its own. A useful cost model has to care for theoretical properties (various definitions of fairness [10]) while taking into account organizational and technology constraints (e.g., granularity of monitoring energy consumption). In NASK, a proprietary cost-splitting scheme has been applied in day-to-day operation. It may serve as good starting point for further customization and development, also as regards the reservation system presented in this paper. In the scheme, lower-level common costs are allocated to higher-level services hierarchically, mostly corresponding the ISO/OSI network layer model. For practical reasons, there are numerous simplifications in the scheme, eg. the cost of maintaining a leased line is averaged for all urban, suburban and rural infrastructures, respectively, resulting in three basic prices of the kilobit-segment accounting unit. Selected details of the model are available on request from the authors of this paper.

Monitoring QoS level of services may be done in various ways, thus generating different load in the network equipment. Limited monitoring functions of network equipment can be enhanced significantly by installing additional software modules which however may adversely influence effectiveness and stability. Another solution is placing additional probes transparently monitoring traffic, however they are costly and may still introduce some additional load to the network. The compromise solution is using as much monitoring functions of network equipment as possible without lowering performance of routers and installing some probes at carefully chosen nodes (e.g., near core routers), which, together with estimation techniques should provide precise picture of the state of the network.

3. System Prototype

A prototype implementing limited set of the proposed system functionality was implemented and tested in NASK laboratory. The development started with preparation of network testbed. Next, monitoring and actuating block were implemented and, finally, application logic elements were added.

3.1. Network Testbed and QoS Mechanisms

The testbed consists of seven routers connected in a way simulating double star topology typical to providers' network. Two routers constitute the redundant core infrastructure, with two edge routers connected from both sides. Other three routers serve as client appliances — connecting two of them to the same edge router creates a potential bottleneck spot. The scheme of the network is depicted in Fig. 2. Cisco 2509 were used for core routers while edge and client routers were Cisco 1720. Using uniform equipment made it easier to implement control and monitoring functions especially after having updated operating system to the same version implementing basic set of DiffServ functionalities (traffic classification, class queues, shaping and policing). Connections between routers are provided via serial interfaces, which allows adjustment of the link speed in broad range up to 2 Mbit/s. Additionally, there are six PCs in the network, three of them hosting traffic generators and simulating users stations, while the other three acting as traffic probes, interconnecting the workstations PCs with the client routers. Control over those three computers is provided via a separate network, not shown in Fig. 2.

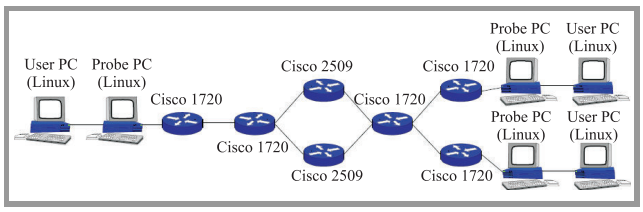


Fig. 2. Testbed topology.

Three service classes were set up in the network: nRT class designed for carrying elastic, mainly TCP traffic, RT class for traffic with strict time requirements, needing low delay and low delay variation, and best-effort class with no quality guarantee. Following DiffServ specification nRT may be associated with one of AF classes and RT is the EF class. These classes were implemented in routers by means of Cisco CBWFQ (nRT and best-effort class) and priority (RT) queues, which allowed minimizing delay thanks to absolute priority over other classes. Client routers were responsible for classifying incoming traffic to classes reflecting contracts, marking and enforcing the guaranteed bitrates by shaping (nRT) and policing (RT). Mean rates of shapers were equal to the rates requested in contracts and buffers were sized proportionally to it (amounting for approximately 1s burst). Marking and policing in client routers provides typical DiffServ scalability as core and edge routers can forward packets analyzing only their DSCP.

Apart from all analogies to the production network it is important to remember about limitations of the testbed resulting from simplified topology and use of basic equipment but also very limited length of links. Specifically, propagation delays in testbed are much smaller, while queuing delays may be, especially during heavy congestion, longer than real. To use such installation efficiently it is necessary to scale experiments, e.g., it is not possible to transmit several HD video streams as link capacity of 2 Mbit/s is several times too small; however after scaling them down to low quality it is possible to send a few streams simultaneously. It is also possible to transmit one stream of better quality and compare results of changing the scale.

3.2. Elements of Monitoring and Actuating Block

To allow monitoring and management of network equipment, a library of communication procedures constituting lower abstraction layer of monitoring and actuating block was developed. Basing on the experience of former projects (e.g., AQUILA) communication via telnet was chosen which, together with using Perl for parsing commands, made library relatively efficient and robust. The procedures are designed primarily for configuring DiffServ-related functions in Cisco routers, however possibility of further adaptation was taken into account by dividing them into two groups. Low level procedures cover basic configuration functions of Cisco routers and are used to provide functionality needed by negotiations block for setting up and managing contracts. This way porting is possible by changing low level procedures only.

Efficiency of implementation, so important when building an on-line system, is however difficult to attain together with reliability as typically network equipment has not been designed with on-the-fly reconfiguration on mind. This makes communication not only time consuming but, worse, it makes verification of configuration difficult – often it is necessary to analyze router output to know if the resulting configuration is consistent. Repeating such pro-

cedure frequently (e.g., after every command sent) introduces unacceptable communication and computing overheads. The solution is performing only basic, mainly syntax, checks frequently and confronting routers configuration periodically with information stored in system database. Basic procedures supporting such verification are part of the library prepared. The functionality of the library supports:

- reading complete configuration of routers,
- sending CLI commands,
- setting clock rates of serial links,
- reading state of interfaces,
- managing access lists,
- managing policers and shapers,
- managing DiffServ AF queues,
- managing route maps,
- managing contracts (i.e., configuring classifiers, queues, shapers or policers etc.),
- reading statistics of queues, shapers, policers, interfaces,
- reading statistics of bandwidth allocated to specific contracts.

3.3. Negotiation and Contracting Logic

Implemented negotiation and contracting algorithms are much simpler than described in Section 2, in fact, the prototype presented in this paper is a proof of concept for the complete reservation system. A rich set of batch programs for managing contracts has been implemented, which use text files to keep track of contracts, and a communication library described in Subsection 3.2 to configure and monitor routers. Specifically, text files are used as the interface between programs, passing information about

- active contracts,
- traffic statistics,
- network topology and traffic engineering paths.

Data access classes are designed so that they can be reused in a future production release of the system, built upon a relational database. Simplifications are acceptable because presented implementation is used only for testing in the laboratory environment; furthermore, implemented programs include some functions which are typical for testing, e.g., program serving contracts not only provides CAC and configuration functions but also, after having successfully set the contract up, it starts traffic generator, thus simulating user activity. In a case when requested contract cannot be served, the system computes estimated time when it is likely that resources will be available and, again, for simplification of experiments reservation program, waits and reissues the request automatically. Another simplification consists in removing expired contracts periodically by searching active contracts. In a real system such solution would lead to extensive computational overhead, and probably accounting errors; it is however acceptable in testbed experiments with limited number of contracts.

CAC functions implemented in negotiation logic use direct feedback from the system to assess the possibility of accepting a contract. First, an appropriate path is selected from statically configured set, then available bandwidth on all links building the path is checked, to find out a bottleneck in a manner similar to RSVP operation [12]. Such a procedure influences scalability obviously, however it is reasonable in the case of centralized control as it allows better utilization of bandwidth than local rules allocating usually preallocated amount of bandwidth [13]. Various measurement-based admission control algorithms use advanced models of aggregate flow, e.g., effective bandwidth [14] and require much attention to extracting precise parameters of both measured aggregate and new flow. Aggregate flow modeling involves collecting difficult to obtain data (e.g., short term averages or peak rates) and complex computations, while estimating parameters of a new flow assumes knowledge of user behavior [15]. The prototype nature of presented system justifies simplifications, specifically, the new contract is admitted after positive evaluation of the following formula:

$$c_{nRT} - \sum_i b_i^* - \gamma \sum_i b_i - \alpha b_{i+1} > 0 \ , \qquad (1)$$

where: c_{nRT} – bandwidth reserved for nRT class, $\sum_i b_i^*$ – bandwidth occupied by all active contracts (read from router statistics), $\sum_i b_i$ – bandwidth requested by all active contracts, b_{i+1} – bandwidth requested by the contract being subject of CAC procedure. Mixing coefficient α allows overbooking (when lower than 1.0), and should be experimentally estimated, while coefficient γ provides some margin over smoothed statistics to be utilized in bursts. In this way it accounts for burstiness and peak rate in a manner similar to used in typical formulations (e.g., [16]) as in experimental set-up buffer size is proportional to average rate declared in the contract. The role of coefficient α is to envisage some level of overbooking at the moment of processing new request, and utilize available capacity more aggressively, which is important in case of limited number of flows. If the formula (1) result is negative the request is blocked and time to wait is computed taking into account parameters of other contracts.

4. Efficiency Tests

Extensive tests were performed to verify various aspects of system architecture and technology used. The following have been checked: efficacy of traffic prioritization,

Table 1
Duration of equipment reconfiguration process

Subject of the test		Number of contracts	Time of setting up [s]		Total time [s]
			first contract	last contract	
Communication library	version 1	100	4	38	2221
	version 2	100	3	6	352
Management program		100	6	9	852

effectiveness of contract management functions, stability of equipment during frequent reconfigurations and CAC algorithms operation.

4.1. Efficiency of Contract Management

The aim of tests was assessment of contracting functions efficiency. The experiments were carried out in two stages: first, the communication library was tested followed by tests of the whole contract management program. In both cases no data were transferred through the network – only requests were processed and routers reconfigured, which allowed measurement of time required to set up the contract by software and equipment. Two versions of contracts setup procedure were tested: the first one adjusts parameters of all already present priority queues while processing every new request, to ensure proportional distribution of bandwidth in nRT class; the second one allocates constant fraction of requested bandwidth, which also results in proportional share and is less time consuming (only one queue is configured each time).
Results of tests are presented in Table 1. Some fluctuations of time were observed, they are probably caused by traffic interference and varying load on the management server. The first version of algorithm is much slower as repeated reconfiguration has computational complexity of $O(n^2)$ for n contracts. Operation of the algorithm in second version is acceptable, it must be however pointed out that periodical recomputing of contracts and reconfiguration of routers may be necessary in case when number of contracts grows over value assumed.
Measurement of execution time for management program was carried out in the similar manner, using second (faster) version of contracting procedures. Setup time overhead introduced by the program is 2 to 5 s and grows with a number of contracts, which is the effect of necessity of analyzing all contracts.

Conclusions. Reconfiguration time is acceptable, however in case of short-time contracts (e.g., lasting several minutes) may be considered annoying by some users. The main limitation lies in routers that process requests sequentially and with limited performance (typically 10 to 15 requests per minute). This time may be shortened by optimization of programs and, first of all, by replacing routers used in testbed with equipment more advanced and better suited for the role (e.g., specialized traffic shapers, etc.). It is also hoped that most reconfiguration actions take place at network edges, being the result of managing requests in a distributed way, and therefore no high request processing volume is required for such a single edge device.

4.2. Possibility of Providing Adequate QoS for nRT Class

Test described in this subsection were devoted to checking ability of providing connections with adequate QoS, namely:

- QoS guarantees in nRT class,
- possibility of bandwidth sharing by nRT and best-effort classes,
- estimating maximum number of contracts which can be served by single router.

It is expected that flows will be transmitted separately with bitrate similar to shaper bandwidth and smoothed by shapers. In periods of limited activity in nRT class best-effort class may occupy additional bandwidth, it should not however influence higher class performance. Estimation of maximum number of contracts supported by routers is crucial to further commercialization of the system, but limitations of equipment used in testbed must be taken into account.
Four experiments were performed, differing in number and type of flows:

- 14 flows, each requesting 128 kbit/s in nRT class,
- 15 flows, each requesting 128 kbit/s in nRT class,
- 14 flows, each requesting 128 kbit/s in nRT class, plus elastic best-effort traffic
- 30 flows, each requesting 64 kbit/s in nRT class.

Contracts were set up prior to traffic generation to prevent configuration disturbing flows. Link rates were configured on 2 Mbit/s level. Four variants of experiments were prepared. In the first variant bandwidth requested by nRT flows is 1792 kbit/s, or 87.5% of total capacity, in the second – 93%. The third variant was designed to test possibility of filling up free bandwidth with best-effort traffic – nRT flows occupied 87.5% of link capacity. The last experiment was devoted to checking maximum number of flows that can be transmitted concurrently.

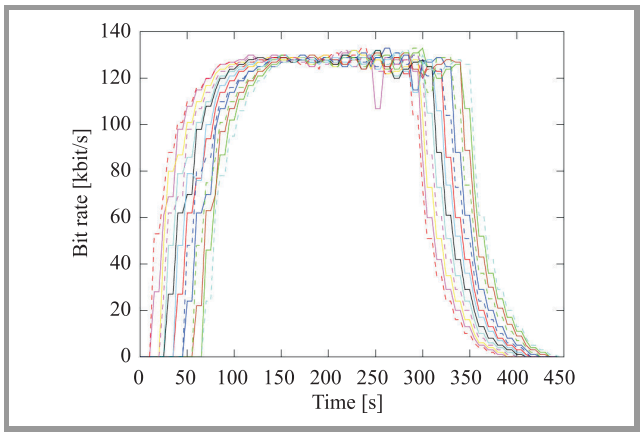


Fig. 3. Average bit rate of 14 nRT flows.

Results of experiments are presented in plots depicting mean bit rates of flows during experiments (30 s intervals were used). Figure 3 reflects results of the first experiment – it may be observed that bandwidth is distributed consistently among flows and guarantees are kept (maximum fluctuations are no higher than 2% which seems to be acceptable for TCP traffic). The second experiment (see Fig. 4) was not so successful – it seems that more than 7% of headroom is necessary to accommodate fluctuations of TCP traffic. The third experiment (see Fig. 5) was

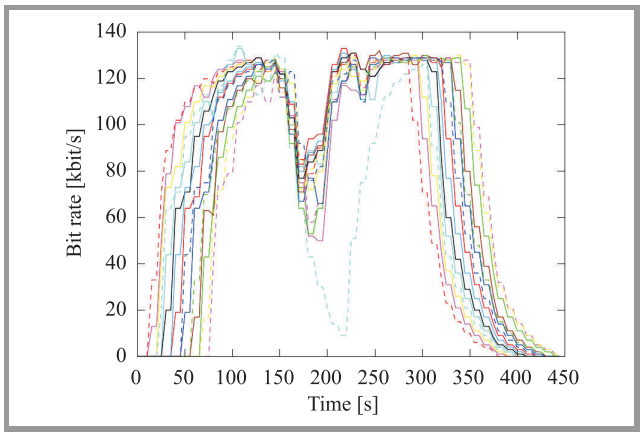


Fig. 4. Average bit rate of 15 nRT flows.

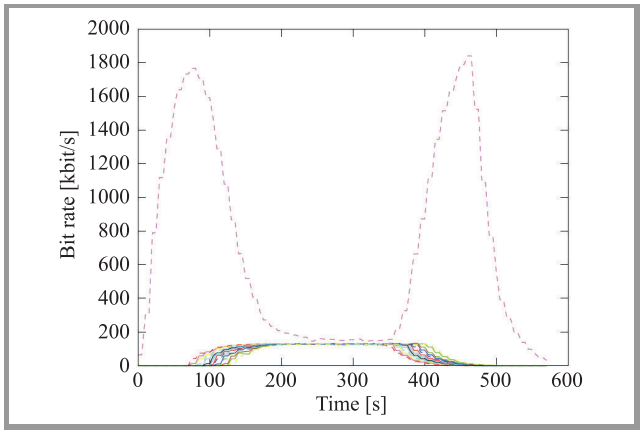


Fig. 5. Average bit rate of 14 nRT flows and best-effort flow.

designed to verify preemptive operation of class queues. It may be observed that best-effort class utilizes link fully when no higher class traffic is generated, however it limits its throughput immediately when first nRT flow has started. Additionally it is worth to notice that existence of best-effort traffic allows higher network utilization than in case of transmitting only QoS guaranteed traffic (1880 kbit/s versus 1792 kbit/s in the first experiment).

The outcome of the last, fourth experiment was negative – transmission was broken due to malfunction of router during setting up approximately twentieth contract. This way it may be estimated that maximum number of class queues and so contracts supported by this lower class Cisco router is some 20.

Conclusions. DiffServ implementation provided in Cisco IOS allows effective prioritization of a limited number of flows. Existence of best-effort traffic not only does not degrade higher classes but also allows better utilization of links. Typical use scenarios and resulting numbers of contracts demanded must be analyzed carefully to define target users of dynamic contracts and select equipment (and so, costs) apt for such an enterprise.

4.3. Analysis of Transient States During Setting up of Contracts

Tests carried out in these group were designed to check possibility of sharing the link by RT and best-effort traffic. Two issues were considered:

– prioritization of RT traffic,

– transient network states caused by configuring new contract and their influence on active contracts.

Possibility of preempting best-effort traffic by UDP RT traffic was tested in experiments. Use of UDP traffic lacking congestion control mechanism allowed credible measurement of packet loss. Checking how QoS parameters of existing contracts change during reconfiguration of routers is important because only when there is virtually no influence, dynamic contracting is possible. Otherwise, when reconfiguration disturbs existing transmission, system applicability will be highly limited.

Table 2
Packet loss rate and delay statistics for UDP priority transmission

		Priority class	
		1 flow	2 flows
Best-effort class	4 flows	**0** *20/39/85*	**1.3** and **7.8** *20/44/86*
	6 flows	**0** *20/42/85*	**6** and **0.5** *20/45/86*

To test prioritizing in RT class, a number of video streams in H.263 format with bit rate 256 kbit/s were transmitted simultaneously. Picture resolution was 176×144 pixels –

the generic setting for mobile phone application. H.263 is CBR codec, however peaks up to 1.4 Mbit/s were observed. During experiments one or two video streams were transmitted in RT class, and four or six in best-effort class. Bandwidth allocated to RT queue was 90% of total link bandwidth. Table 2 presents video streams parameters: percentage of packet loss in subsequent transmissions in bold face, and total delay statistics for priority traffic in italics (minimum/mean/maximum delay in ms).

Conclusions. Tests confirmed that priority traffic is transmitted correctly. In case of a single flow no packets are lost and delay is kept at acceptable level. Some fluctuations of delay show that packets are successfully buffered which prevents dropping. When two flows are sent simultaneously some loss may be observed which is result of using relatively short queue (8 packets). Short queue however limits maximum delay to the level similar as in case of one stream. Very limited influence of best-effort traffic must be noted which makes the tested routers a good choice when real time traffic prioritizing is needed.

The following experiment aimed investigating transient states which can occur during reconfiguring routers to set up new contract. It was suspected that additional load to the router caused by its reconfiguration may influence existing contracts. To verify this, packet loss and delay during reconfiguration were carefully observed. Test traffic consisted of 6 VoIP streams transmitted in best-effort class and 3 identical streams in RT class. All streams use G.723.1 protocol sending frames of 24 B every 30 ms. To test the impact of router reconfiguration, an additional fourth contract is set up after 200 s from starting the first nine ones. Setting up contract comprises all activities from registering it in contract base to configuring access list in the routers. After completing these tasks transmission is started in 210th second from beginning of the experiment.

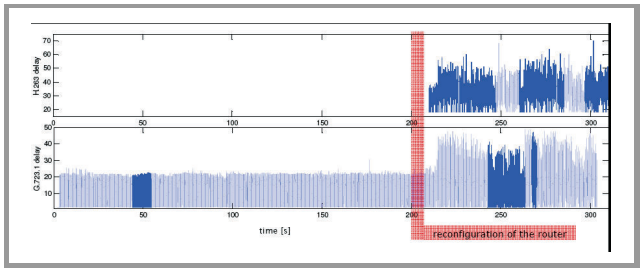


Fig. 6. Delay of original 3 VoIP transmissions (lower graph) and additional VoIP transmission (upper graph).

Figure 6 presents results of the experiment. Lower graph depicts delay of first three VoIP streams sent in RT class while in the upper graph delay of additional fourth transmission may be observed. Thanks to the delay between reconfiguration ($t = 200$ s) and start of transmission ($t = 210$ s) it may be easily noticed that reconfiguration influences delay in negligible degree. After starting fourth stream delay grows significantly due to higher load, however it still remains on appropriate level (well below 100 ms).

Conclusions. Reconfiguration of the router does not influence data transmission, so dynamic contracting is possible provided the router is not overloaded. In case of overload configuration functions (*management plane*) are influenced first than data forwarding (*data plane*).

4.4. Admission Control Algorithm

The subject of the test was checking strategy of contract admission described in Subsection 3.3. and tuning its parameters. The aim of this algorithm is maximizing network utilization while keeping QoS guarantees in nRT class. As flows transmitted in nRT class use TCP protocol, main aim is providing mean bit rate close to requested value. The typical use of such a service may be WWW browsing, which in turn may be modeled by *on-off* generator with exponential *off* periods and Pareto sizes of data to transmit. Two sets of generator parameters were used during the experiment:

1. $k = 1.2$, $o = 512$ kbit/s, $\lambda = 2$ – mean bit rate approx. 70 kbit/s,
2. $k = 1.2$, $o = 512$ kbit/s, $\lambda = 5$ – mean bit rate approx. 200 kbit/s.

The k parameter is shape coefficient of Pareto distribution[2], o is maximum bit rate of generated flow and λ is inverse of mean *off* time. In both experiments 30 contracts lasting 300 s are requested every 5 s. Each of them requests 512 kbit/s which is its peak rate. Total declared bandwidth (15 Mbit/s) exceeds available bandwidth set to 2 Mbit/s. Actual total mean bandwidth of all contracts is much lower. It is 2.1 Mbit/s in the first and 6 Mbit/s in the second case, however is still beyond available bandwidth limit, so for correct functioning of the network efficient admission control mechanism is necessary.

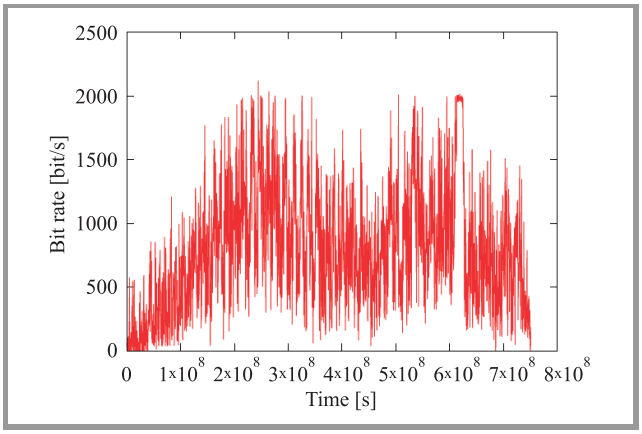


Fig. 7. Short term average bit rate for traffic generated with first set of parameters.

Figures 7 and 8 present average bit rate graphs of traffic captured on the interface of receiving machine during

[2]Pareto distribution PDF: $f(x) = kx_m^k/x^{k+1}$. Parameter x_m is in both cases equal 1200 B which seems to be reasonable estimate of minimum amount of data sent in single transmission.

the first variant of experiment. Averaging period was 0.3 s and 30 s respectively. Both graphs show the decrease of bit rate in the middle of the experiment, which is the result of postponing of nearly half of contracts for 300 s, so they could start after completion of the first group. Short term averages show huge burstiness of traffic, which for a short while reaches the declared maximum. Analysis of graph with longer averaging period reveals that network is not fully utilized (in fact 15 active contracts need $15 \cdot 70$ kbit/s = 1.05 Mbit/s) and parameters of admission mechanism seem to be too conservative. It must be noted however that in terms of declared bandwidth network offers high degree of overbooking – 15 active contracts means that $15 \cdot 512$ kbit/s = 7.68 Mbit/s were simultaneously contracted, while 2 Mbit/s were available.

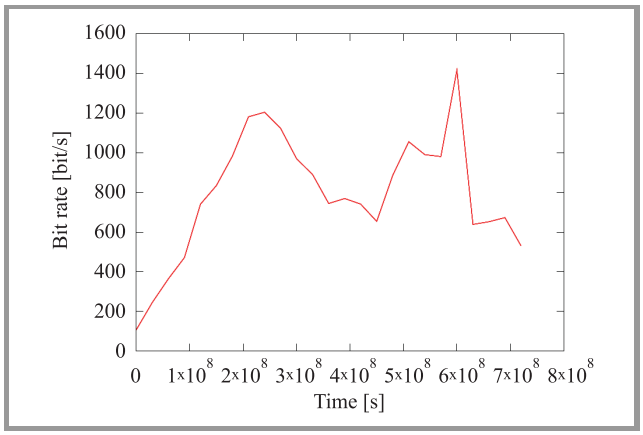


Fig. 8. Long term average bit rate for traffic generated with first set of parameters.

Bit rates observed while executing the second version of the experiment are depicted in Fig. 9 and 10. Again, short (0.3 s) and long (30 s) term average bit rates are presented. Similarly to the first variant, nearly half of contracts were postponed, however generated bit rates were much higher. By comparing long-term averages it is easily noticeable that number of accepted contracts is much too high, which results in congestion. In case of such overload by bursty traffic admission strategy is too liberal, which results not only in limiting bandwidth of flows, but also in its unfair distribution among contracts (flow bit rates span from 30 kbit/s to 150 kbit/s).

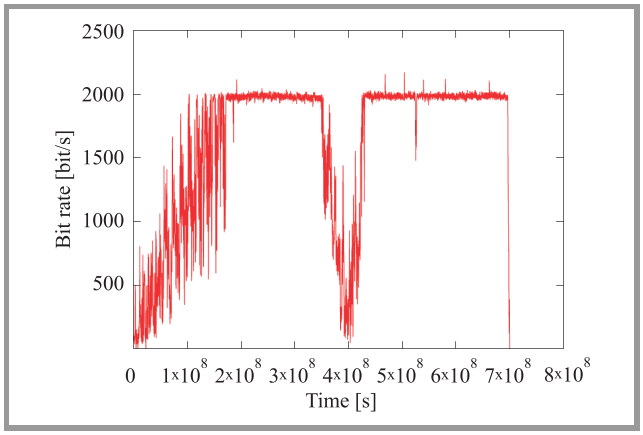


Fig. 9. Short term average bit rate for traffic generated with second set of parameters.

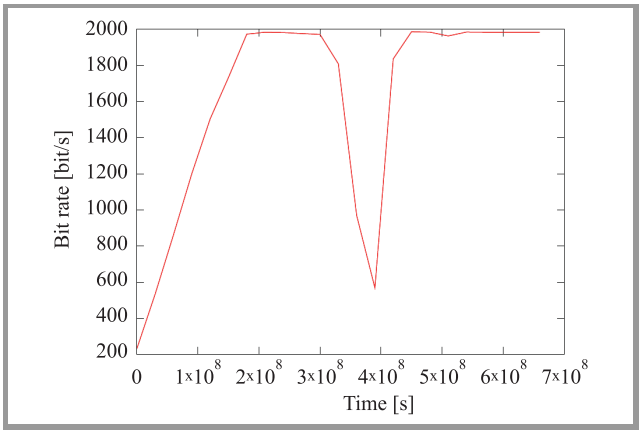


Fig. 10. Long term average bit rate for traffic generated with second set of parameters.

Conclusions. Efficient admission control using model (1) with constant coefficients for various kinds of traffic is impossible. Additional problem is using 30 s averages to monitor network state which introduces too much delay in control loop (in analyzed case new request arrived every 5 s).

5. Summary

Experiments performed were designed to check main prerequisites of dynamic QoS contract management system, namely:

- efficiency of DiffServ flow prioritizing under heavy load of offered traffic and configuration commands,
- ability of network equipment to frequent reconfiguring of contracts,
- applicability of admission algorithm proposed.

In authors' opinion results of tests are optimistic and justify continuation of the work: even relatively simple equipment allows to efficiently configure and prioritize contracts. Data and management planes are appropriately separated and do not influence each other. The number of contracts supported is limited, however it is reasonable for serving a household.

Tests also revealed weak points, those being slow and unreliable communication with routers, limitation of simultaneously active queues and difficulty of CAC algorithm tuning. The efficiency of configuring the equipment may be improved by implementing some functions in parallel and providing better algorithms for checking configuration and monitoring network parameters (switching to communication via SNMP may be helpful). To build heavily loaded system equipment of greater efficiency (and possibly different technology) is however necessary. On the other hand

improvement of admission strategy is possible mainly by modification of algorithms by:

- estimating real bit rates between measurements (it may be done by including input from contract database),
- introducing additional parameters determining traffic characteristic into contract request (e.g., some measures of burstiness) to tune algorithm parameters individually,
- providing more QoS classes to make traffic transmitted in particular class more consistent.

Summing up, the existing technology allows to implement the system providing dynamic contracts with QoS guarantees. Neither existing networks structure nor scalability and amount of work necessary to develop such a system constitutes major obstacle in its implementation and introduction. Furthermore, such a system will naturally assist operators in offering new services to users, it could also be attractive to users offering them quality guarantees contracted dynamically, so (probably) cheaper than today. The real problem is no real need for such services observed on the market.

Acknowledgement

The paper was partially supported by Polish Ministry of Science and Higher Education grants N N514 416934 and PBZ-MNiSW-02/II/2007.

References

[1] X. Wang and H. Schulzrinne, "RNAP: a framework for congestion-based pricing and charging for adaptive multimedia applications", *IEEE J. Sel. Areas Commun.*, vol. 18, no. 12, pp. 2514–2529, 2000.

[2] M. Howarth (Ed.), "Initial Specification of Protocols and Algorithms for Inter-domain SLS Management and Traffic Engineering for QoS-based IP Service Delivery and their Test Requirements", Deliverable D1.2,MESCAL, 2004.

[3] D. Goderis (Ed.), "Functional Architecture Definition and Top Level Design", Deliverable D1.1, TEQUILA, 2000.

[4] J. Enríquez and J. Andrés (Eds.), "Definition of Business, Communication and QoS models – Intermediate", Deliverable D.1.1, EuQOS, 2005.

[5] P. Arabas, M. Kamola, K. Malinowski, and M. Małowidzki, "Pricing for IP networks and services", *Inform., Knowl., Sys. Manag.*, vol. 2, pp. 153–171, 2003.

[6] I. Constantiou (Ed.), "ISP Business Model Report", Deliverable 7.1, M3I, 2002.

[7] "IP Solution Center – MPLS VPN", white paper, Cisco Inc., 2003.

[8] F. P. Kelly, "Notes on effective bandwidths", in *Stochastic Networks: Theory and Applications*, F. P. Kelly, S. Zachary, I. B. Ziedins, Eds. Oxford University Press, 1996, pp. 141–168.

[9] NS2 [Online]. Available: http://www.isi.edu/nsnam/ns

[10] C. Courcoubetis and R. Weber, *Pricing Communication Networks: Economics, Technology and Modelling.* Chichester: Wiley, 2003.

[11] G. L. Lilien, P. Kotler, K. S. Moorthy, *Marketing Models*. Prentice Hall, 1992.

[12] R. Braden (Ed.), "Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification", RFC 2205, 1997.

[13] A. Bak, W. Burakowski, F. Ricciato, S. Salsano, and H. Tarasiuk, "Traffic handling in AQUILA QoS IP network", in *Quality of Future Internet services* of *Lecture Notes in Computer Science 2156*, Springer 2001.

[14] J. Ko, "A decision theoretic approach to measurement-based admission control", in *Proc. IEEE Int. Conf. Commun. ICC-2007*, Glasgow, Scotland, 2007, pp. 742–747.

[15] K. Kanonakis, H. Leligou, and T. Orphanoudakis, "Online flow characterisation for measurement-based admission control: a practical perspective", *Int. J. Res. Rev. Comput. Sci.*, vol. 1, no. 4, pp. 149–157, 2010.

[16] S. Floyd, "Comments on Measurement-based Admission Control for Controlled-Load Services", Tech. Rep., 1996.

Piotr Arabas received his Ph.D. in computer science from the Warsaw University of Technology, Poland, in 2004. Currently he is assistant professor at Institute of Control and Computation Engineering at the Warsaw University of Technology. Since 2002 with Research and Academic Computer Network (NASK). His research area focuses on modeling computer networks, predictive control and hierarchical systems.

e-mail: parabas@ia.pw.edu.pl
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

e-mail: Piotr.Arabas@nask.pl
Research Academic Computer Network (NASK)
Wąwozowa st 18
02-796 Warsaw, Poland

Mariusz Kamola received his Ph.D. in computer science from the Warsaw University of Technology, Poland, in 2004. Currently he is assistant professor at Institute of Control and Computation Engineering at the Warsaw University of Technology. Since 2002 with Research and Academic Computer Network (NASK). His research area focuses on economics of computer networks and large scale systems.

e-mail: mkamola@ia.pw.edu.pl
Institute of Control and Computation Engineering
Warsaw University of Technology
Nowowiejska st 15/19
00-665 Warsaw, Poland

e-mail: Mariusz.Kamola@nask.pl
Research Academic Computer Network (NASK)
Wąwozowa st 18
02-796 Warsaw, Poland

Tutorial

GPON, the Ultimate Pertinent of Next Generation Triple-play Bandwidth Resolution

D. M. S. Sultan[a] and Md. Taslim Arefin[b]

[a] *Chalmers University of Technology, Gothenburg, Sweden*
[b] *Daffodil International University, Dhanmondi, Bangladesh*

Abstract—Optical transmission is getting more popular in the access network due to the increasing demand for bandwidth. New services like IP television (IPTV) transmission, video on demand (VoD) etc. over Internet together along high speed Internet access are confronting the demand of higher bandwidth at the customer end in today's Ethernet network backbone. Even though today's well deployed XDSL (i.e., VDSL/VDSL2+, SHDSL) solutions can satisfy bandwidth demand but are limited to the restriction regarding distance. Hereby, the suitable solution for high bandwidth demand with a long reach can be met by reaching optical cable to customer end directly. One of the possible ways would be to install passive optical network (PON). Gigabit PON (GPON) is the far-most advanced PON solution used by European and US providers while providers in Asia predominantly use EPON/GePON. This GPON is the basic technology to support the structure of the next-generation fiber to the home (FTTH) system. This paper provides an overview of such GPON solution associating its network architecture, transmission mechanisms and some key services.

Keywords—FTTH, Gigabit PON (GPON), IPTV, OLT, ONU, PON, VOIP.

1. Introduction

In today's increasingly competitive and technologically advanced telecom environment, broadband networks offer telecom operators both new business opportunities and new challenges. Carriers are now confronted with some problems: customer losing, revenue decreasing, investment risk, high operational expense (OPEX), etc. At the same time, subscribers need more suitable services, more personalized applications with high bandwidth consumption as well as quicker troubleshooting to support a vast array of voice/data/internet services. Carriers must resolve these issues in the stages of constructing, operating and upgrading their networks by deploying gigabit passive optic network (GPON) of today.

Along with increasing requirements of broadband access from residential customer and business customer, broadband access network has become urgent constructing network to carrier. Fiber technique has become mainstream and mature technique to develop broadband access. The growth of fiber to the home (FTTH) subscribers also gives an opportunity to deliver value-added services (viz. triple play solution such as Internet, voice and video) on the same infrastructure based on the new FTTH architecture.

The subscribers' requirements on the bandwidth keeps growing, so application of purely fibers in the access network are the direction for broadband development, and the FTTH solution becomes the focus of the operators in developing the network. As per today's telecom market, all telecom vendors provide optical line terminal (OLT) that would smoothly inherit the GPON access but also support the ADSL2+, VDSL2, and voice over IP [1]. So far evaluated GPON solution by all vendors like Huawei, Ericsson, and Motorola etc. is such a unified and powerful platform that not only provides FTTx (fiber to the home, building, curb, node, etc.) solution but also provides the option to merge into next generation network (NGN) platform of fixed mobile convergence concept. Besides, advanced GPON solution of today is not only complying with FTTH, but also amenable with fiber to the curb (FTTC), to fiber to the building (FTTB) in case of some specific scenarios.

Currently, GPON interfaces can transmit services over passive optical fibers at a symmetrical bit rate of 1.25 Gbit/s or an asymmetrical bit rate of 2.5 Gbit/s downstream and 1.25 Gbit/s upstream for a distance of 20 km. In downstream, GPON OLT transmits encrypted user traffics over the shared bandwidth. In upstream, it uses time division multiple access (TDMA) technology to provide shared high-bit-rate bandwidth. Meanwhile, GPON OLT supports dynamic broadband algorithm, making the distribution of bandwidth to optical network unit (ONU) more flexible [2], [3]. In a glance, this paper aims to represent the GPON's competence of meeting the constant rising triple play bandwidth demand to next generation broadband solution architects.

2. GPON Architecture

In core GPON solution, the OLT is placed in the central office to provide the GPON access mode; splitters at the entrance of the residential block or near the management office of the residential block. For the FTTH, ONT series are provided directly in the multimedia box of each subscriber. For the FTTB, the remote ONU could be placed near the building to support ADSL2+, VDSL2, G.SHDSL

technologies to utilize the existing twisted pair resource. All equipments are directly connected with optical fibers. The integrated access platform OLT realizes the flexible access infrastructure depending on the different scenario to operator requirement.

Also, all of the equipments including the OLT, optical network unit/multi dwelling unit (ONU/MDU) and ONT can be managed by the broadband network management server to realize the end to end management solution. A total GPON architecture is shown in Fig. 1 amenable with NGN and Internet platform.

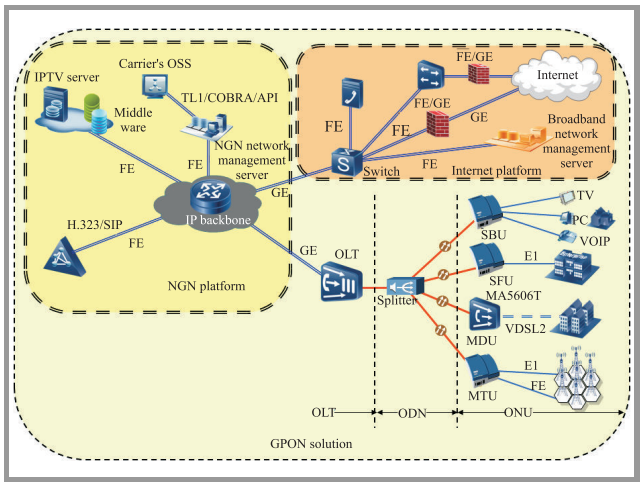


Fig. 1. GPON architecture along with NGN and Internet platform.

For business subscribers and individuals who accept the shared optical channel and a guaranteed bandwidth of less than 100 Mbit/s, the point to multipoint (P2MP) fiber access technology, which is based on the GPON, is an ideal choice. When the GPON is adopted, the bandwidth allocation of each subscriber could be flexible adjusted as per splitting ratio. So far 1:64 ratio is popular in GPON deployment, thus the average guaranteed bandwidth for each subscriber can reach up to 39 Mbit/s. So, bandwidth requirements for various broadband services, such as high-definition IPTV, can be satisfied.

When subscribers are dispersed and each requires a large guaranteed bandwidth and extreme private optical channel, the P2P fiber access technology can be adopted. The P2P scheme can meet the large bandwidth requirements of high-value subscribers and so as can be treated as a premier substitution of choice for high-value business subscribers, such as banks.

3. Why GPON?

In evolution from P2P to PON technologies, APON, BPON, EPON, GPON and WDM-PON named several PON technologies have been come from industrial and academics research collaboration yet. Among them two rival technologies are EPON and GPON. Regarding incessant requirement of bandwidth, next generation PON would be 10GEPON, WDM-PON or Hybrid WDM/TDM-PON and a comparative summary among the PON technologies are shown in Table 1.

In EPON, both downstream and upstream line rates are 1.25 Gbit/s but due to the employment of 8 B/10 B line encoding, the bit rate for data transmission is of 1 Gbit/s only. On the other hand, in GPON, several upstream and downstream rates are specified up to 2.48832 Gbit/s, since GPON standard is defined in the ITU-T G.984.x series of recommendations [5] and it refers the bit rates of the conventional TDM systems. Guard time is the time between two neighboring time slots used for differentiating the transmission from various ONUs. In EPON, it is composed of laser on-off time, automatic gain control (AGC) and clock-and-data recovery (CDR). IEEE 802.3ah standard [6] has specified values (classes) for AGC and CDR but in GPON, guard time consists of laser on-off time, preamble and delimiter. According to the ITU-T G.984 recommendation, GPON has obviously shorter guard time than EPON [2]. However, it requires stricter physical layer constraints than EPON. Multi-point control protocol (MPCP) is implemented at the medium access control (MAC) layer in EPON to perform the bandwidth allocation, auto-discovery process and ranging. Two control messages, REPORT and GATE are used for defining dynamic bandwidth allocation [6]. Normally, a GATE message carries the granted bandwidth information from the OLT to an ONU in the downstream direction, while a REPORT message is used by an ONU to report the bandwidth request to the OLT in the upstream direction. This message exchange allows the time slots to be assigned according to the traffic demand of each individual ONU depending upon the available bandwidth. The size of REPORT and GATE message is 64 B which is equal to the shortest Ethernet frame. Furthermore, the EPON standard does not support frame fragmentation. Both OLT and ONUs can directly send and receive Ethernet frames with variable length.

In the contrary, GPON guard time is based on the standard of 125 μs periodicity. This periodicity provides significant advantages compared to EPON. Messages, such as control, buffer report and grant messages can be efficiently integrated into the header of each 125 μs frame. In order to pack Ethernet frames into the 125 μs frame, Ethernet frame fragmentation has been introduced as well in GPON. Within GPON, each Ethernet frame or frame fragment is up to 1518 B and is encapsulated in a general encapsulation method (GEM) frame where GEM header is of 5 B. Status report message in GPON DBA process is known as the overhead that requires 2 B. Upstream QoS awareness has also been integrated in the GPON standard with an introduction of the concept of transport containers (T-CONTs). T-CONT represents a class of service. Hence, GPON can provide a simple and efficient means for setting up a system for multiple service classes. Saying all these comparative technical issues of GPON and EPON comparative analysis, it could be sum up that GPON clearly leading forward than EPON to the current context.

Table 1
A comparative presentation among different PONs [4]

	A/BPON	EPON (GEPON)	GPON	10GEPON	WDM PON
Standard	ITU-T G.983	IEEE 802.3ah	ITU-T G.984	IEEE 802.3av	ITU-T G.983
Data packet cell size	53 B	1518 B	53 to 1518 B	1518 B	Independent
Maximum downstream line rate	622 Mbit/s	1.2 Gbit/s	2.4 Gbit/s	IP 2.4 Gbit/s Broadcast 5 Gbit/s On demand 2.5 Gbit/s	1–10 Gbit/s per channel
Maximum upstream line rate	155/622 Mbit/s	1.2 Gbit/s	1.2Gbit/s	2.5 Gbit/s	1–10 Gbit/s per channel
Downstream wavelength	1490 and 1550 nm	1550 nm	1490 and 1550 nm	1550 nm	Individual wavelength/channel
Upstream wavelength	1310 nm	1310 nm	1310 nm	1310 nm	Individual wavelength/channel
Traffic modes	ATM	Ethernet	ATM Ethernet or TDM	Ethernet	Protocol independent
Voice	ATM	VoIP	TDM	VoIP	Independent
Video	1550 nm overlay	1550 nm overlay/IP	1550 nm overlay/IP	IP	1550 nm overlay/IP
Max PON splits	32	32	64	128	16/100's
Max distance coverage	20 km	20 km	60 km	10 km	20 km
Avg. bandwidth per unit	20 Mbit/s	60 Mbit/s	40 Mbit/s	20 Mbit/s	up to 10 Gbit/s

Even though GPON infrastructure is the most beneficial PON solution of today in terms of performance, matured recommendation from authorized society (i.e., ITU-T, FSAN and IEEE) and more revenue in long-run among other PONs, it still lacks behind of proper bandwidth utilization in terms of all possible applied scenarios for being TDM based. To support the fact, several types of next generation PON (viz. 10GEPON, WDM-PON, XL-PON etc.) are still being standardized. Among them, the most competitive solution would be WDM-PON that uses WDM technology instead of TDM at the physical interface. It uses a single feeder fiber to take advantage of the same economics associated with traditional PONs; but logically, WDM-PON uses a point-to-point architecture. Therefore, it is far more scalable and secure than other PONs. Today, WDM-PON delivers 20 Gbit/s per fiber (1.25 Gbit/s dedicated per user on a 1:16 split). In addition, WDM-PON enables a dedicated wavelength for each user, ensuring the security that SMBs demand and providing greater provisioning flexibility – essentially, WDM-PON is a fat pipe that can support Ethernet, Metro Ethernet or TDM, depending on what the provider wants to offer. Within the next two years, WDM-PON will offer 80 Gbit/s per fiber probably, which will allow 2.5 Gbit/s per subscriber on a 32:1 split. Besides, WDM-PON is also less expensive to deploy, maintain and upgrade. For example, it uses colorless optics, which eliminates the sparing issue associated with typical DWDM network elements. In addition, if a bandwidth upgrade becomes available with better line terminals and network terminals, the provider can simply upgrade these without affecting service for existing customers. Also, WDM-PON channel plan changes can be accommodated simply by swapping the arrayed wavelength grating (AWG) at the OLT and remote splitter, rather than having to pull new fiber or replace the terminals themselves. Considering functionality and scalability, it seems that WDM-PON seems like the obvious upgrade path for GPON but WDM-PON still facing some hurdles like the function of density. While this density mirrors GPON, the OLT must increase the feeder fiber count to increase the subscriber count from 16 today to 640 subscribers or more in the future [7]. Hereby, although WDM-PON is significantly (four to five times) less expensive per Mbit/s, it is currently about three to four times the cost of GPON on a per-subscriber basis.

4. GPON Features

4.1. Operating Wavelength

The operating wavelength range is about 1500 nm for the downstream and 1350 nm for the upstream. In addition a wavelength range 1550–1560 nm can be used for downstream RF video distribution.

4.2. Open Bandwidth Allocation

Both, static bandwidth allocation (SBA) as well as dynamic bandwidth allocation (DBA) can be implemented in GPON networks. SBA guarantees fixed bandwidth for each ONU whereas DBA guarantees the dynamic bandwidth allocation for each ONU in accordance to users' requests.

Basically, DBA is a process for consenting quick adoption of user-end bandwidth allocation based on current traffic need. Hereby, OLT controls the whole DBA process that allocates the bandwidth to ONUs. This process works only in upstream whereas downstream traffic is just been broadcasted.

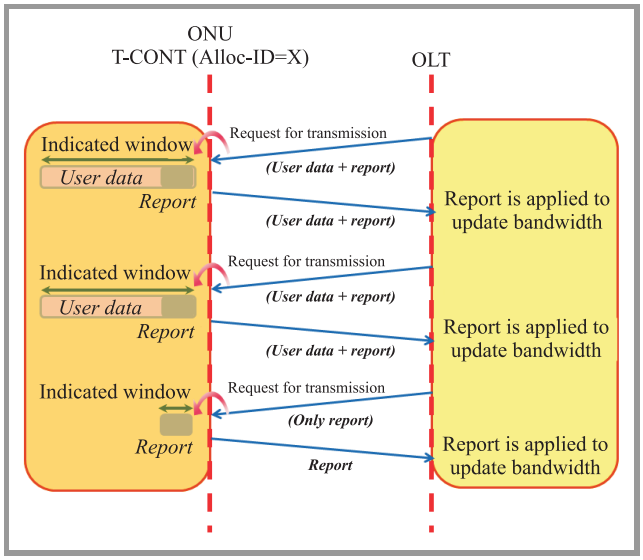


Fig. 2. DBA process.

Figure 2 shows a typical DBA process. To determine the quantity of traffic allocate to an ONU, the OLT needs to know the traffic status of the T-CONT associated with the ONU. In status reporting method, a T-CONT indicates the quantity of packets that are waiting in its buffer. Once the OLT receive this information, it can reapportion the grants to various ONUs accordingly. If an ONU has no information waiting to be transported, a grant is sent to an idle cell upstream upon receiving for indicating that the buffer is empty. Hence, this informs the OLT that the grant for that T-CONT can be assigned to other T-CONTs. Besides, if an ONU has a long queue waiting in the buffer, the OLT can assign multiple T-CONTs to that ONU [8].

4.3. Emmence Downstream Efficiency

GPON can provide the downstream efficiency up to ∼92% since non encoded non return to zero (NRZ) is applied [2]. The ∼8% efficiency is mitigates by use of overhead. IP-based standard definition TV (SDTV, needs ∼3 Mbit/s BW) and particularly high-definition TV (HDTV, needs ∼18 Mbit/s BW) services are now the increasing demand of today's customer.

It is seen that GPON can provide guarantee of high speed internet subscription for 278 users (Fig. 3) even if the video content goes 100% HDTV with 50 video channels on PON because of its efficient 2,488 Mbit/s downstream transport [9].

Likewise, for a single family unit network with multiple dwelling unit (MDU) application of splitting ratio of 1:32, GPON is capable for proving basic high speed internet service along VOIP/SDTV/HDTV services to 32 ONU supporting 8 subscriber each (viz. 278/32). Eventhough the number of this subscription can be even more depending upon technical and business practice of service provider.

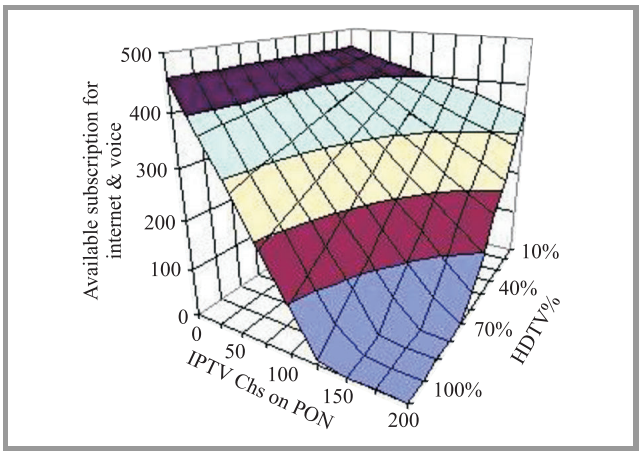


Fig. 3. Available flawless subscription for SDTV and HDTV application in GPON interface [9].

4.4. Gauranted QoS at Upstream

Triple play services (Internet, voice and video) require a solid backbone of QoS mechanism where GPON is a right candidate as it is enhanced with PON layer mechanism that goes beyond layer 2 Ethernet and layer 3 IP class of service (CoS) to ensure the delivery of high quality voice, video and TDM data over TDMA based shared media. However, GPON upstream rate is ∼1.25 Gbit/s that is 20% higher in comparison to EPON but its state of art QoS architecture makes different from other competing solutions existing today. GPON uses an out-of-band bandwidth allocation map with the concept of traffic containers (T-CONTs) that ensure upstream-granted entity. The downstream and upstream frame timing is 8 kHz at standard telecom where services are encapsulated into frames in their innate format by a process called GPON encapsulation mode (GEM). GPON also supports protection switching in less than 50 ms like SONET/SDH.

GPON is enhanced with unique low-latency capability is that all upstream TDMA bursts from all ONUs can occur within an 8 kHz frame (i.e., 125 μs) as illustrated in above figure (Fig. 4). Each downstream frame comprises of an efficient bandwidth allocation map that is broadcasted to all ONUs and supported a fine granularity of bandwidth allocation. This so called out-of-band mechanism aids the GPON DBA to sustenance very small grant cycles without conceding bandwidth utilization.

Basically, T-CONTs are a PON-layer mechanism for upstream QoS whereas CoS is determined by layer 2 or layer 3 methods that use the same T-CONT type. Here, voice services are assigned to a voice T-CONT at ONU and best-effort data are assigned to best-effort T-CONTs. DBA confirms that T-CONTs using a higher CoS, like voice, get priority access on the PON and preempt T-CONTs with lower CoS, such as Internet data. T-CONT size and timing

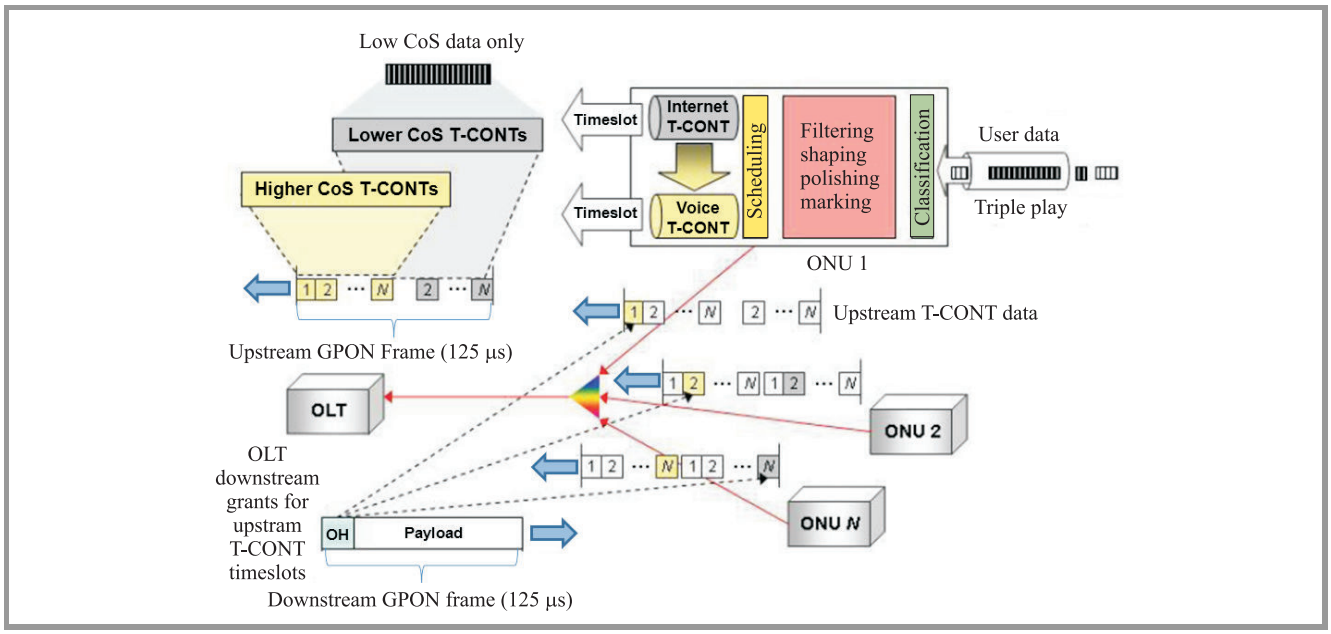


Fig. 4. GPON QoS/CoS capability that enriched with fragmented payloads.

are then allocated on the PON by the OLT based on the CoS demands and resources in PON [9].

However, GEM also aids the fragmented payloads so as a low-CoS T-CONT can stop its upstream burst in the middle of a payload, may allow a higher-CoS T-CONT its access and then resume its transmission when told to by the DBA mechanism. Therefore, large bursts of low-priority, best-effort data will have minimal effect on high-priority, delay-sensitive traffic (i.e., voice and TDM) in a highly utilized PON.

4.5. Security

In GPON, downstream data are broadcasted to all ONUs and every ONU has allocated time when data belongs to it, as like TDM. For this reason some malicious user can reprogram their own ONU and can capture all the downstream data belong to all ONUs connected to that OLT. In upstream, GPON uses point to point connection so that all traffic is secured from eavesdropping. Therefore, each of confidential upstream information (such as security key) can be sent in clear text.

Thus in GPON, transmission layer specification (G.948.3) describes the use of an information security mechanism to ensure that users are allowed to access only the data intended for them. The encryption algorithm to be used is the advanced encryption standard (AES). It accepts 128, 192 and 256 byte keys which makes encryption extremely difficult to compromise. A key can be changed periodically without disturbing the information flow to enhance security [8].

4.6. Boosted with Interoperability

GPON standard is closed developed monitor by FSAN and ITU-T that clearly indicates its feasibility of wide convergence. GPON is still capable for providing a constant satisfactory transmission performance by use of CoS T-CONT assignments in integration to TDM circuit emulation service (CES) as well as ATM technology.

5. Key Triple-play Service Solutions with GPON

5.1. Voice Solution

GPON VoIP access service solution shown in Fig. 5, household user side adopts ONU with built-in VOIP function; Data service is directly accessed to IP network via MA5680T OLT [10]. In order to ensure the quality of voice service, GPON system and upper layer IP network need to support IP QOS, to perform the scheduling with higher priority on VOIP voice message.

GPON system is able to meet QoS requirement of different services through the means such as service flow

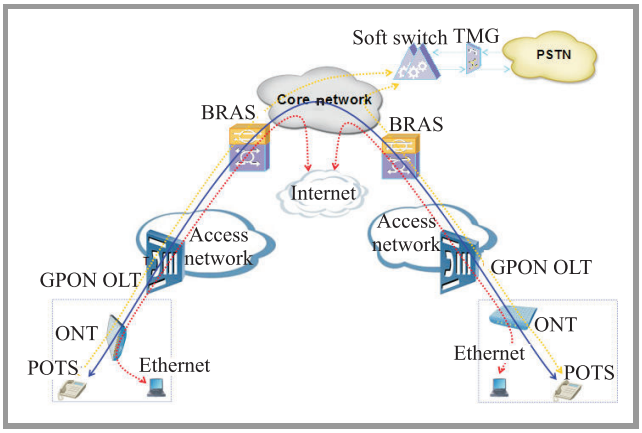


Fig. 5. GPON system VoIP solution.

classification, measurement, marking, and multi queuing mechanism, queue scheduling, buffer management, congestion handling, etc. GPON OLT performs the identification based on the user flow and bandwidth management in case of QoS handling of user flow entrance, to realize the management on the user at the network entrance, and classify the different services, by using one or multiple queuing scheduling methods to meet the requirements of QoS. The upper layer equipment marks the priority from the message of network downlink. In GPON OLT, the system can perform queuing scheduling and bandwidth management according to the marks.

5.2. Internet Access Solution

Two standard solutions can be adopted for implementing internet access solution over GPON. One of them could to wholesale the point to point protocol over Ethernet (PPPoE) subscribers to the ISPs, which is commonly known as virtual local area network (VLAN) stacking multi-ISP wholesale Internet access solution. This solution is more suitable for Internet service wholesale to large ISPs where each of them own BRAS. In the solution, the GPON platform performs the following functions:

– identifying different ISPs,

– performing traffic isolation between ISPs,

– identifying subscribers,

– performing traffic isolation between subscribers,

– implementing PPPoE access.

This method is suitable for Internet service wholesale to large ISPs.
Another one is to adopt layer 2 tunneling protocol (L2TP). In this solution, the carrier's broadband remote access server (BRAS) supports L2TP access concentrator (LAC), while each ISP provides the L2TP network server (LNS). L2TP tunnels are set up between the LAC and the LNS. Subscribers are accessed via PPPoE. This solution is more suitable for Internet service wholesale among small ISPs. In some scenarios like Internet service provisioning for business subscribers, Internet protocol over Ethernet (IPoE) dedicated line access is recommended and in this instance, GPON system guarantees the QoS. However, GPON may also establish VPNs with the upstream carrier's PE equipment.

5.2.1. VLAN Stacking Multi-ISP Wholesale Internet Access Solution

Hereby, GPON OLT adopts 802.1Q VLAN tagging for subscriber identification to enable multi-ISP wholesale access. The outer VLAN is used for ISP identification, and the inner VLAN is used for identification of subscribers that are to be sent to the BRAS for authentication. PPPoE are adopted for subscriber access, as it is shown in Fig. 6.

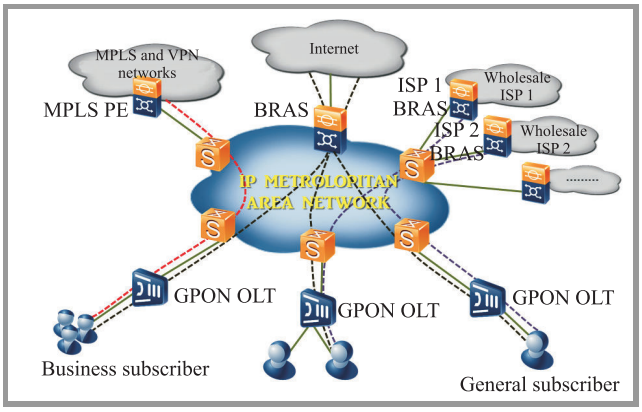


Fig. 6. Wholesale subscriber access via VLAN stacking.

According to Fig. 6, wholesale ISP subscribers do access internet via VLAN stacking. Each wholesale subscriber has two layers of VLAN tags. The outer VLAN tag is used for ISP identification. It is reported to the ISP BRAS after being transparently through the layer 2 metropolitan area network (MAN). The inner VLAN tag is used for identification of ISP wholesale subscribers. Each subscriber is identified via an inner VLAN tag. The ISP BRAS will first extract the outer VLAN tag and implement PPPoE authentication. After that, the ISP BRAS complete the authentication via binding between the inner VLAN and the subscriber account. When the number of ISP subscribers exceeds limit (i.e., 4000), another outer VLAN layer can be assigned to the ISPs, so each outer VLAN can supports access subscribers within limit.
GPON OLTs are capable to work in VLAN stacking mode and common mode. When a GPON OLT port is work in VLAN stacking mode, after having received untagged packets, the OLT will insert two layers of VLAN tags to the packets and then send them upstream. The outer VLAN tag is used for ISP identification, while the inner VLAN tag is used for subscriber identification. And in common mode, the two layers of VLAN tags is used in combination for subscriber identification. VLAN stacking mode and common mode can coexist on most vendors provided GPON OLTs, where packet switching and forwarding are implemented based on the outer VLAN tag.

5.2.2. L2TP Multi-ISP Wholesale Internet Access Solution

In this solution (Fig. 7), the Internet access subscribers on the GPON are connected to the carrier's BRAS via PPPoE. The BRAS serves as the LAC as defined in L2TP to set up L2TP tunnels with LNSs of various ISPs. The BRAS is able to identify subscribers of different ISPs based on the VLAN tag contained in the GPON subscriber packet, or based on the domain name contained in the subscriber

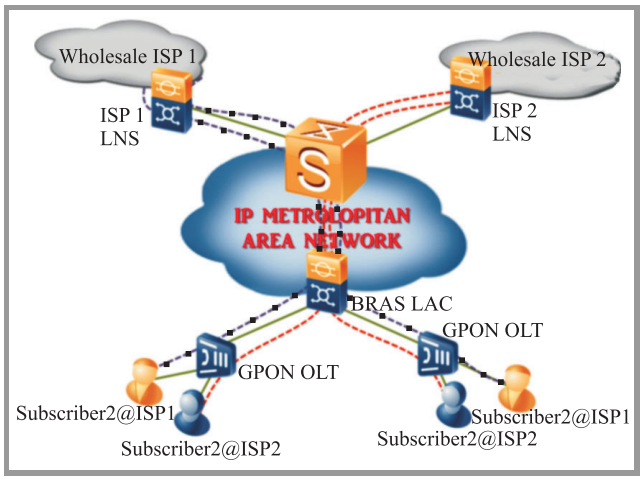


Fig. 7. Internet access L2TP using PPPoE.

account. It then accesses subscribers of different ISPs to the corresponding ISPs through different L2TP tunnels.

5.3. GPON IP Based Video Service Solution

The provisioning of GPON IP based video services is implemented by electronic program guide (EPG)/content portal. When an STB starts and passes authentication, it acquires an IP address. With the address, it accesses the video system to perform software load and user authentication. When it passes user authentication, the video management system will send an EPG according to his/her rights and service subscription. EPG is portal pages through which the subscriber can select services. There are many ways to acquire an EPG with assistance from the client on an STB and EPG/portal server. For BTV services, an EPG should offer necessary multicast session information such as multicast address, port no., media type, and coding scheme. Coding schemes for IPTV programs include the MPEG2, MPEG4, and WMV. The MPEG2 provides ordinary video quality at a code rate of 2 Mbit/s and broadcasting-class video quality at a rate of 3.5 Mbit/s∼4 Mbit/s. The more advanced MPEG4/H.264 provides higher video compression ratios. The MPEG-4 enables high video quality at a rate of 1.5 Mbit/s while H.264 can provide more video services with higher definition at rates below 1 Mbit/s. Video streams are delivered using MPEG over IP [11]. Multicast video streams coming from the coder and video server are directly output to core network and then sent to subscribers via a FTTP access network.

IPTV that is already been emerged with many IP based broadband services, is continuously evolving and changing. At the same time, service providers' networks have different needs depending on markets, distribution areas, plant and density. Increasingly, service providers need access platforms to launch service from different points in the network, to utilize different copper or fiber facilities, and to incorporate more quality and performance with the services offered. Adaptability becomes an important aspect for access to meet a variety of needs, with the choice in the hands of the service provider rather than dictated by the limitations of technology.

GPON optical network terminal (ONT) provides support for high speed data and high definition IPTV service with Gigabit Ethernet ports (see Fig. 1). It is a cost effective solution for point to multipoint scenarios where passive optical splitters are used to allow a single optical fiber for providing multiple premises. IPTV delivers video services based on IP multicast. At the source end, different program, sources are configured with different multicast address, and reach the ONU device through a series of broadcast service. Effective broadcast IPTV service requires extensive bandwidth and the support of IP multicast and IGMP. For deployments requiring open access or other multiple broadcast sources, these can be provisioned on VLAN basis. Thus, through IGMP and IP multicast, the ONT model provides full support for broadcast IPTV services with VLAN capability supporting open access IPTV solutions. The large bandwidth available on such GPON ONTs enables them to transparent transport all video encoding standards, including MPEG-2 and MPEG-4. In example, if each ONT supports over 256 multicast MPEG-2 video channels concurrently, then that is capable to provide virtually unlimited video streams support with unicast MPEG-2. Additionally, some ONTs (i.e., enablence ONTG4000i) are ideally suited to support VoD, PPV and other IPTV related packet-based services desired today by numerous network operators [12], [13].

6. Conclusion

In conclusion, GPON solution is expecting a robust, capable, reliable, cost-effective platform that yet been standardized by ITU-T and FSAN as well as being enhanced with ongoing research conducting at industry and academy. But it can be deployed today at access network architecture, so as to offer the end users more bandwidth to meet the demand of new services which will in turn generate more revenues and act as a baseline for the newer technologies to develop.

References

[1] "Gigabit-Capable Passive Optical Networks (GPON): General Characteristics", ITU-T/G.984.1 [Online]. Available: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.984.1-200803-I!!PDFE&type=items and http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.984.1-200910-I!Amd1!PDF-E&type=items.

[2] "Gigabit-capable Passive Optical Networks (GPON): Physical Media Dependent (PMD) layer specification", ITU-T/G.984.2, 2010 [Online]. Available: http://www.itu.int/rec/

[3] "Gigabit-capable Passive Optical Networks (G-PON): Transmission convergence layer specification", ITU-T/G.984.3 [Online]. Available: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.984.3-200803-I!!PDF-E&type=items

[4] B. Skubic, J. Chen, J. Ahmed, L. Wosinska, and B. Mukherjee, "A comparison of dynamic bandwidth allocation for EPON, GPON and next generation TDM PON", *IEEE Commun. Mag.*, vol. 47, issue 3, pp. 40–48, 2009.

[5] ITU-T G.984.x [Online]. Available: http://www.itu.int/rec/TREC-G/e

[6] IEEE 802.3ah [Online]. Available: http://www.ieee802.org/3/efm

[7] C. Bock *et al*., "Architecture of future access networks", in *Next-Generation FTTH Passive Optical Networks*, J. Prat, Ed. New York: Springer, 2008.

[8] I. Cale, A. Salihovic, and M. Ivekovic, "Gigabit passive optical network-GPON", *Inf. Technol. Interfaces*, pp. 679–684, June 2007.

[9] "GPON is more than just a faster PON", 2010 [Online]. Available: http://www.broadlight.com/docs/pdfs/wp-gpon-more-than-faster-pon.pdf

[10] "Solution – broader access bandwidth comies true", Huawei Technologies LTD., 2010 [Online]. Available: http://www.huawei.com/publications/view.do?id=690&cid=342&pid=61

[11] M. Abrams and A. Maislos, "Insights on delivering an IP triple play over GE-PON and GPON", in *Proc. Opt. Fiber Commun. Conf. OFC 2006*, Anheim, USA, 2006.

[12] Enablence ONTG4000i, "Advanced Indoor GPON ONT for next generation Networks", 2010 [Online]. Available: http://www.enablence.com/media/pdf/951_00240_ont_g4000i_data_sheet _rev_1.0_17feb2010.pdf

[13] "Gigabit-capable passive optical networks (G-PON): ONT management and control interface specification", ITU-T G.984.4, 2010 [Online]. Available: http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-G.984.4-200802-I!!PDF-E&type=items

D. M. S. Sultan received his B.Sc. in computer engineering from American International University Bangladesh in 2005. Soon he joined as a lecturer, CSE faculty in University of Development Alternative. In 2006, he has been awarded as PBX administrator in extend Broadband, Turkish Republic of North Cyprus. Afterwards, he was an Assistant Product Engineer, Huawei Technologies (Bangladesh) Ltd in 2007. In 2010, he has achieved his M.Sc. in communication engineering major in electrical engineering – specialization research from Chalmers University of Technology, Sweden. Currently, he is working as Research Student at Photonics Laboratory, MC2.
e-mail: sultan@alumni.chalmers.se
Photonics Laboratory
MC2 Chalmers University of Technology
SE 41296, Gothenburg, Sweden

Md. Taslim Arefin received his B.Sc. in computer engineering from American International University Bangladesh in 2005. Afterwards, he joined University of Development Alternative as a Lecturer, CSE department. He pursued his M.Sc. in electrical engineering – specialization telecommunications from Blekinge Institute of Technology, Sweden in 2008. At latest, he is working as Senior Lecturer in the Dept. of ETE at Daffodil International University, Dhaka, Bangladesh.
e-mail: arefin@daffodilvarsity.edu.bd
Department of Electronics
and Telecommunication Engineering
Daffodil International University
Dhanmondi, Dhaka-1209, Bangladesh

Paper

Developing a Secure Image Steganographic System Using TPVD Adaptive LSB Matching Revisited Algorithm for Maximizing the Embedding Rate

P. Mohan Kumar[a] and K. L. Shanmuganathan[b]

[a] CSE Department, Jeppiaar Engineering College, Chennai, India
[b] CSE Department, R.M.K. Engineering College, Chennai, India

Abstract—Steganography is the approach for hiding any secret message in a variety of multimedia carriers like images, audio or video files. Whenever we are hiding a data, it is very important to make it invisible, so that it could be protected. A number of steganographic algorithms have been proposed based on this property of a steganographic system. This paper concentrates on integrating Tri way pixel value differencing approach and LSB matching revisited. The secret data embedded in images were images, text and audio signals so far. The proposed scheme has also come with the executable file as secret data. Also, the experimentation results show that, the important properties of a steganographic system such as imperceptibility, capacity of the carrier image and also resistance against the various steganalytic tools have also been achieved with this stego-system.

Keywords—executable file, LSBMR, spatial domain, steganalysis, TPVD.

1. Introduction

The term steganography means the science of hidden communication. The way in which steganography differs from another secure data communication technique called cryptography is, the visibility of the data exchange. In cryptography, even though the actual data transaction may not be known to a third person, he may get a doubt that some abnormal or suspicious communication is taking place. But, in case of steganography, the hidden communication will never come to the notice of the eavesdropper. Because, the carrier signal we are using to hide the secret data is going to be innocent. So, we can call the technique as information hiding [1]–[4].

Another technique which is based on the information hiding strategy is digital watermarking. But, in case of digital watermarking, the important property of information hiding known as resistance to removal is preferred. So, in these applications, we are not worrying about imperceptibility but resistance to removal. This is mainly used in commercial applications like copyright protection of digital forms of media like video or image. Unlike image steganography, digital watermarking techniques mainly concentrate on keeping logos or any other symbols or images in the carrier data. And also it is made sure that those signals embedded are not able to be removed by any other person. There are a number of watermarking techniques have been explained in [5]–[7].

For a long period of time many researchers have been involved in developing new steganographic systems. Meanwhile, the development of steganalytic tools are also started growing. Steganalysis is a process of finding the existence of a secret data in a cover media [8]. Whenever a suspicious image is received, the main task of a steganalytic tool is to find the algorithm used for hiding secret data in the image. Most of the steganographic algorithm developers are also trying to crack their own algorithm using the existing steganalytic tools, so that the strength and weaknesses of their system may be found.

2. Related Work

Generally, digital image steganography is a way to exchange secret data. So, the important components of a steganographic system include an embedding/extracting algorithm, secret key which is going to be shared by the sender and receiver of the secret data and also a communication channel which is considered to be more secure [9]. The general frame work for a steganographic system is shown in Fig. 1.

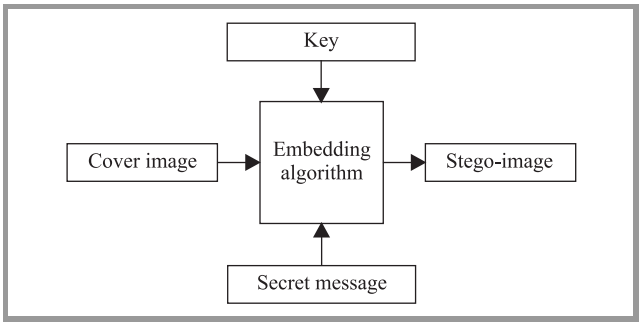


Fig. 1. A simple image steganography scheme.

This framework has been derived from the popular idea called prisoner's problem [9]. In this approach Alice and Bob were trying to exchange an escape plan without the knowledge of the warden. Some of the terms used in steganographic system are cover-media (the digital media which is used to hide secret data), secret data (the important data to be hidden) and stego-media (after embedding the secret message in the cover media). The hidden data cannot be detectable when we are performing the embedding phase randomly and also the level of independence between the secret message and cover as well as stego objects [10]. There are many other ways for providing more security includes the usage of encryption-decryption functions for embedding and extraction of secret data [11]. Since JPEG images are widely exchanged through internet, choosing JPEG image for sending secret message to the receiver will never be suspicious. And also, the redundancies that are appearing in JPEG images help us to hide more information securely. Methods for improving the hiding capacity of a JPEG image have been explained in [12].

The least significant bits replacement method or LSB method is the very simple and a commonly used approach for developing steganographic system. Because the amount of space that an image can provide for hiding data will be more comparing with other algorithms. And also the implementation of this technique is also very easy. In this approach, the image pixel's LSB is replaced by one bit of secret data [13]. Spatial domain embedding technique is also known as image domain. The techniques that are following spatial domain embedding are embedding the secret message in the intensity of the cover image pixels. Spatial domain techniques include bit-wise methods that apply bit insertion and noise manipulation techniques [14]. The main disadvantage of LSB replacement is that, while hiding secret data in the image, some of the pixels will never be modified or replaced with the secret bits, since we are using pseudo random generator for placing the secret message bits. As a result, very simple steganalytic tool could trace the existence of the secret message.

But this problem of asymmetry can easily be avoided by an alternate scheme using a LSB matching scheme. In this technique, if the secret bit is not matching with the LSB of cover image, then ±1 will be added randomly. By doing so, we can reduce the probability of increase or decrease in the pixel value modification can be avoided. So, we can eliminate the problem we faced in LSB replacement technique. Also, the steganalytic algorithms which can find the stego-images which were obtained from LSB replacement technique cannot find the stego-images we got from LSB matching.

There are several steganalytic algorithms found for finding stego-images which were got by LSBM (LSB matching) technique. In [15], the image is being taken and its two least significant bit planes are considered. The bit planes are split into 3×3 overlapped sub images. According to the number of gray levels those sub images are classified. In one sub image, the LSBM is applied and found that the alteration rate of cover image is higher than that of stego-image. In [16], the authors have compared the function of LSBM to a low pass filter through the histogram of the image. They found that the number of high frequency components is very less comparing to the original cover image. But later in [17], this method is found that it will not be working well in case of gray scale images. As a remedy, the author has proposed techniques using down-sampled image and adjacency histogram instead of traditional histogram.

Instead of handling pixel values independently, the other technique proposed by Jarno in [18], is using a pair of pixels for embedding which is known as LSBM revisited (LSBMR). In this technique, the author has proposed an approach for data hiding, in which the LSB of the first pixel carries one bit of information, and a function of the two pixel values carries another bit of information. So, in this approach the changes that are made in the cover image are very few. Also, the modification rates of pixels have been greatly reduced. But all the techniques analyzed above are not taking care of the relationship between the pixel and its neighborhood.

There are many data embedding schemes analyzed which are taking the relationship of a pixel to its neighbor. In [19], a hiding scheme has been proposed by replacing the LSB of a cover according to the difference values between a pixel and its four touching neighbors. This method uses the edges of an image for hiding secret data. Although this method can achieve more visually imperceptible stego-images, the security performance is poor. Since the method just modifies the LSB of image pixels when hiding data, it can be easily detected by existing steganalytic algorithms.

The pixel value differencing is another type of edge based data hiding scheme, which has been proposed in [20], in which the number of embedded bits is determined by the difference between a pixel and its neighbor. If there is large difference between the pixels, the number of secret bits that can be embedded will also be large. Also based on the experimental results, this approach can provide a larger embedding capacity.

Executable file structure

The program loader that is a subset of the Windows system assumes the loading executable files into a virtual memory, so the executable files have the format that the program loader can identify, and the format is called portable executable (PE). It is necessary to know the PE format and RVA which is an address type used in the PE in order to understand the new methods for hiding information in the PE. The system uses an image file as a cover to embed it to an executable program or an executable file for the proposed system.

The characteristics of the executable file does not have a standard size, like other files, for example the image file (BMP) the size of this file is between (2–10 MB). Other example is the text file (TEXT) the size often is less than 2 MB. Through the characteristics of files have been

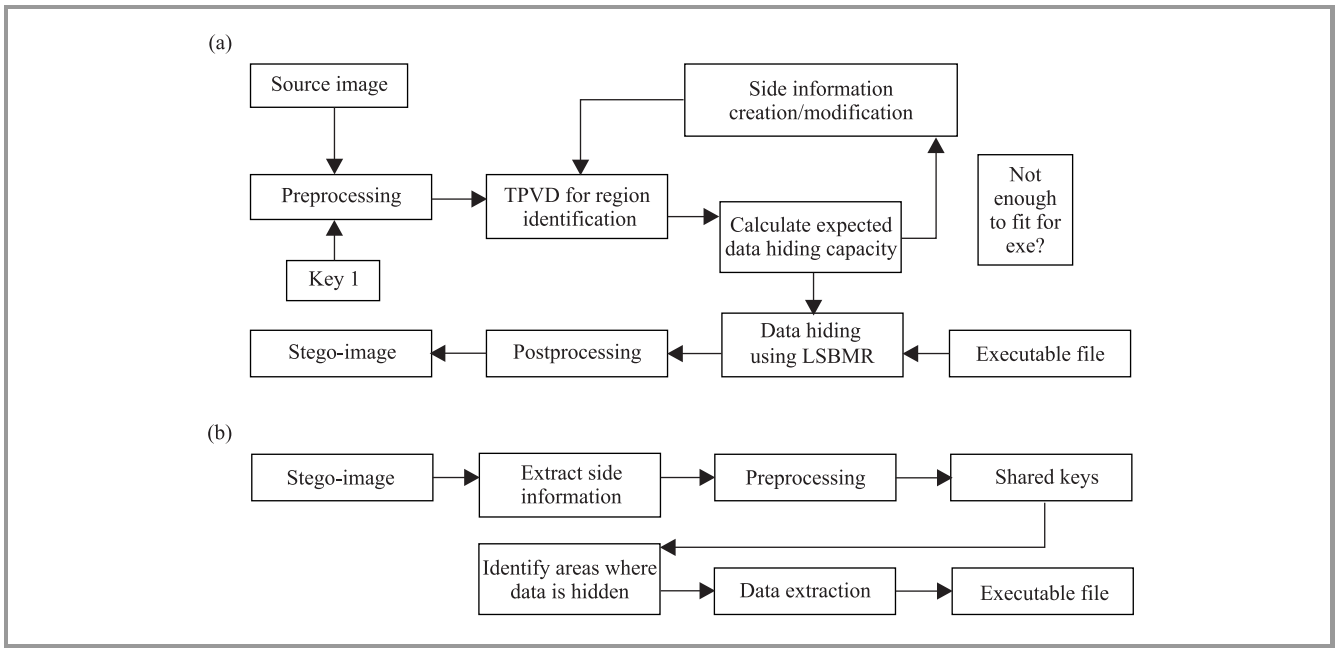


Fig. 2. Proposed executable file (a) embedding architecture and (b) extraction architecture.

used as a hidden information's, it found that lacks sufficient size to serve. For these features of the Executable file, it has unspecified size; it can be 650 MB like window setup file or 12 MB such as installation file of multi-media players. For taking advantage of this feature make it a suitable environment for concealing information without detect the file from attacker and discover the hidden information in stego-image.

A PE file section represents code or data of some sort. While code is just code, there are multiple types of data. Besides read/write program data (such as global variables), other types of data in sections include application program interface (API) import and export tables, resources, and relocations. Each section has its own set of in-memory attributes, including whether the section contains code, whether it's read-only or read/write, and whether the data in the section is shared between all processes using the executable file. Sections have two alignment values, one within the desk file and the other in memory. The PE file header specifies both of these values, which can differ. Each section starts at an offset that's some multiple of the alignment value.

3. Proposed System

The architecture for embedding phase of the proposed system is shown in Fig. 2a. The proposed system initializes some parameters, which are used for subsequent data preprocessing and region selection, and then estimates the capacity of those selected regions. If the regions are large enough for hiding the given secret message, then data hiding is performed on the selected regions. Finally, it does some postprocessing to obtain the stego-image. Otherwise the scheme needs to revise the parameters, and then repeats region selection and capacity estimation until can be embedded completely. Please note that the parameters may be different for different image content and secret message. We need them as side information to guarantee the validity of data extraction. In practice, such side information (7 bits in our work) can be embedded into a predetermined region of the image. In data extraction, the scheme first extracts the side information from the stego-image. Based on the side information, it then does some preprocessing and identifies the regions that have been used for data hiding. Finally, it obtains the secret message according to the corresponding extraction algorithm. In this paper, we apply such a region adaptive scheme to the spatial LSB domain. We use the absolute difference between two adjacent pixels as the criterion for region selection, and use LSBMR as the data hiding algorithm. The details of the data embedding and data extraction algorithms are as follows.

Data embedding

1. The cover image of size of m×n is first divided into non-overlapping blocks of 2×2 pixels. For each small block, we rotate it by a random degree in the range of $\{0, 90, 180, 270\}$, which is decided by a key which is decided by the user.

2. The resulting pixel blocks are $P(x, y)$, $P(x+1, y)$, $P(x, y+1)$ and $P(x+1, y+1)$. Consider the pixel $P(x,y)$ as the current pixel, consider the pixel pairs as $P1$, $P2$ and $P3$, where:

$$P1 = (P(x,y), P(x, y+1)),$$
$$P2 = (P(x,y), P(x+1, y)),$$
$$P3 = (P(x,y), P(x+1, y+1)).$$

3. Calculate the difference values for the pixel pairs keeping one pixel as the current pixel.

4. Find the appropriate range from the range table to identify the region or the pair of pixels (assume as x_i and x_{i+1} in which the secret data is going to be embedded.

5. We deal with the above embedding units in a pseudo-random order determined by a secret key. For each unit (x_i, x_{i+1}), we perform the data hiding according to the following four cases:

   (1) $\mathrm{LSB}(x_i) = m_i$ and $f(x_i, x_{i+1}) = m_{i+1}$ and $(x'_i, x'_{i+1}) = (x_i, x_{i+1})$,

   (2) $\mathrm{LSB}(x_i) = m_i$ and $f(x_i, x_{i+1}) \neq m_{i+1}$ and $(x'_i, x'_{i+1}) = (x_i, x_{i+1} + r)$,

   (3) $\mathrm{LSB}(x_i) \neq m_i$ and $f(x_{i-1}, x_{i+1}) = m_{i+1}$ and $(x'_i, x'_{i+1}) = (x_{i-1}, x_{i+1})$,

   (4) $\mathrm{LSB}(x_i) \neq m_i$ and $f(x_{i-1}, x_{i+1}) \neq m_{i+1}$ and $(x'_i, x'_{i+1}) = (x_{i+1}, x_{i+1})$,

   where m_i and m_{i+1} denote two secret bits to be embedded.

6. After data hiding, the resulting image is divided into non-overlapping 2×2 blocks. The blocks are then rotated by a random number of degrees based on key.

Data extraction

The architecture of the proposed system for executable file extraction is shown in Fig. 2b.

1. Partition the stego-image into 2×2 pixel blocks.

2. Calculate the difference values as we did in embedding phase.

3. Find the embedding location and then rotate by random degrees which is decided by the secret key.

4. Until all the hidden bits are extracted completely, go through all the pixel blocks whose difference is greater than or equal to the available cut-off value. This cut-off value will be the maximum value of the pixel that could be used for embedding data.

4. Experimental Results and Analysis

One of the important properties of our steganographic method is that it can first choose the sharper edge regions for data hiding according to the size of the secret message by adjusting a cut off value. As explained in the paper, the larger the number of secret bits to be embedded, the smaller the cut off becomes, which means that more embedding units with lower gradients in the cover image can be released. When is 0, all the embedding units within the cover become available. In such a case, our method can achieve the maximum embedding capacity of 100% (100% means 1 bpp on average for all the methods in this paper), and therefore, the embedding capacity of our proposed method is almost the same as the LSBM and LSBMR methods except for 7 additional bits. One of the sample cover image taken for the experimentation and the corresponding stego-image with executable file are shown

Fig. 3. Cover image (a) and (b) stego-image using proposed approach.

in Fig. 3. There are no visual artifacts found in the stego-image so that the stego image is having the hidden exe file which could not be identified by the human visual system (HVS). A comparison of accuracy of RS features between the existing and proposed methods are provided in Table 1. In Fig. 4, the LSB planes of the cover image and

Table 1
Average accuracy [%] of RS features set on FLD

Embedding rate methods	10%	20%	30%	40%	50%
Existing	88	91	94	98	99
Proposed	51	52	51	50	53

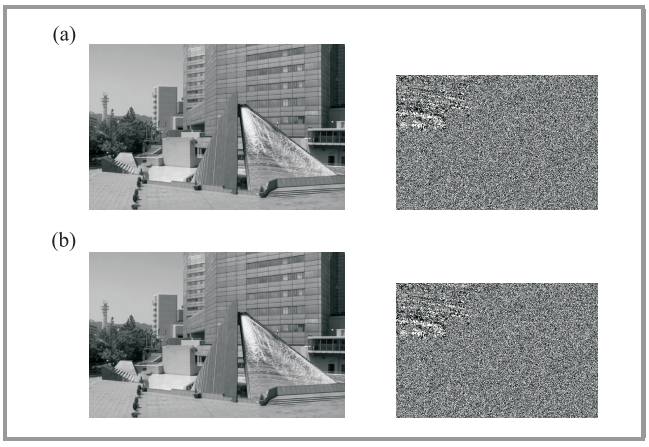


Fig. 4. The LSB planes of (a) the cover image and (b) the stego-image.

stego-image are given. Based on the histogram analysis the cover image could not be suspected so that this method is producing stego images which will not be traced by the existing steganalytic algorithms. Table 2 contains the data

Table 2
Data for drawing ROC curves

False positive rate	0	0.1	0.2	0.3	0.5
True positive rate	0.3	0.5	0.6	0.65	0.7

for drawing ROC curves and RS diagram for the proposed system in comparison with the existing system is shown in Fig. 5.

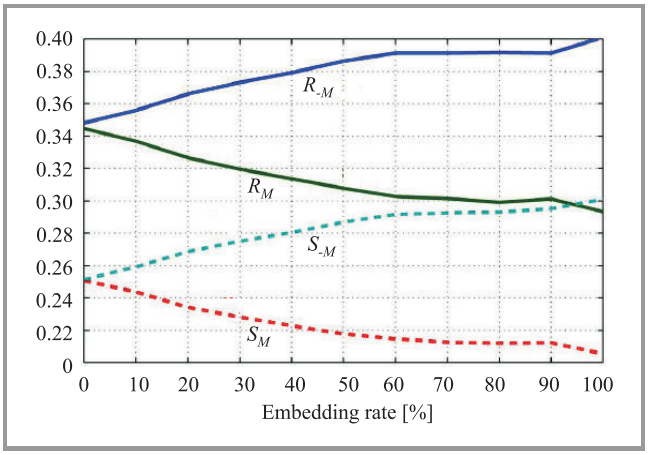


Fig. 5. RS diagram for proposed method.

5. Conclusion

In this paper, an image steganographic scheme in the spatial LSB domain is studied in which an edge based scheme also included. Normally, there exist some smooth regions in natural images, which would cause the LSB of cover images not to be completely random or even to contain some texture information just like those in higher bit planes. If embedding a message in these regions, the LSB of stego-images becomes more random, and according to our analysis and extensive experiments, it is easier to detect. In most previous steganographic schemes, however, the pixel/pixel-pair selection is mainly determined by a PRNG without considering the relationship between the characteristics of content regions and the size of the secret message to be embedded, which means that those smooth/flat regions will be also contaminated by such a random selection scheme even if there are many available edge regions with good hiding characteristics. The experimental results evaluated on thousands of natural images using different kinds of steganalytic algorithms show that both visual quality and security of our stego-images are improved significantly compared to typical LSB-based approaches and their edge adaptive versions. Furthermore, it is expected that our adaptive idea can be extended to other steganographic methods such as audio/video steganography in the spatial or frequency domains when the embedding rate is less than the maximal amount.

References

[1] N. Provos and P. Honeyman, "Hide and seek: an introduction to steganography", *IEEE Sec. Priv. Mag.*, vol. 1, no. 3, pp. 32–44, 2003.

[2] J. Fridrich, "Applications of data hiding in digital images", in *Proc. Int. Symp. Sign. Process. Apl.*, Brisbone, Australia, 1999, pp. 22–25.

[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding – a survey", *Proc. IEEE*, vol. 87, no. 7, pp. 1062–1078, 1999.

[4] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding", *IBM Syst. J.*, vol. 35, no. 3–4, pp. 313–336, 1996.

[5] M. Swanson, M. Kobayashi, and A. Tewfik, "Multimedia data embedding and watermarking technologies", *IEEE Proc.*, vol. 86, no. 6, pp. 1064–1087, 1998.

[6] I. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia", in *Proc. First Int. Worksh. Inf. Hiding*, R. Anderson, Ed. Cambridge: Springer, 1996, pp. 183–206.

[7] I. J. Cox, M. L. Miller, and J.A . Bloom, *Digital Watermarking*. Morgan Kaufmann, 2002.

[8] T. Pevný and J. Fridrich, Multiclass detector of current steganographic methods for JPEG format, *IEEE Trans. Inf. Forensics Sec.*, vol. 3, no. 4, pp. 635–650, 2008.

[9] G. Simmons," The prisoner's problem and the subliminal channel, *CRYPTO*, pp. 51–67, 1983.

[10] J. Zollner and H. Federrath, "Modelling the security of steganographic systems", in *Proc. 2nd Inf. Hiding Worksh.*, Portland, USA, 1998, pp. 345–355.

[11] N. J. Hopper, J. Langford, and L. Von Ahn, "Provably secure steganography", in *Advances in Cryptology: CRYPTO 2002*. Springer, 2002.

[12] L. Zhang, H. Wang, and R. Wu, "A high capacity steganography scheme for JPEG 2000 baseline system", *IEEE Trans. Image Process.*, vol. 18, no. 8, 2009.

[13] T. Morkel, J. H. P. Eloff, and M. S. Olivier, "An overview of image steganography" [Online]. Available: http://mo.co.za/open/stegoverview.pdf

[14] N.F. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software", in *Proc. 2nd Inf. Hiding Worksh.*, Portland, USA, 1998.

[15] F. Huang, B. Li, and J. Huang, "Attack LSB matching steganography by counting alteration rate of the number of neighbourhood gray levels", in *Proc. IEEE Int. Conf. Image Process.*, San Antonio, USA, 2007, vol. 1, pp. 401–404.

[16] J. Harmsen and W. Pearlman, "Steganalysis of additive-noise modelable information hiding", in *Proc. SPIE Electronic Imaging*, Santa Clara, USA, 2003, vol. 5020, pp. 131–142.

[17] A. D. Ker, "Steganalysis of LSB matching in grayscale images", *IEEE Sig. Process. Lett.*, vol. 12, no. 6, pp. 441–444, 2005.

[18] J. Mielikainen, "LSB matching revisited", *IEEE Sig. Process. Lett.*, vol. 13, no. 5, pp. 285–287, 2006.

[19] K. Hempstalk, "Hiding behind corners: using edges in images for better steganography", in *Proc. Comput. Women's Congress*, Hamilton, New Zealand, 2006.

[20] D. Wu and W. Tsai, "A steganographic method for images by pixel-value differencing", *Pattern Recognit. Lett.*, vol. 24, pp. 1613–1626, 2003.

P. Mohan Kumar, B.E., M.E., Ph.D., works as Associate Professor in Jeppiaar Engineering College and he has more than 8 years of teaching experience. His areas of specializations are Network security, Image processing and artificial intelligence.

e-mail: mohankumarmohan@gmail.com
Jeppiaar Engineering College
Chennai, India

K. L. Shanmuganathan, B.E, M.E., M.Sc., Ph.D., works as the Professor and Head of CSE Department of RMK Engineering College, Chennai, Tamil-Nadu, India. He has more than 18 years of teaching experience and his areas of specializations are Artificial Intelligence, Computer Networks and DBMS.

e-mail: kls_nathan@yahoo.com
R.M.K. Engineering College
Chennai, India

Paper

An Efficient Chaotic Interleaver for Image Transmission over IEEE 802.15.4 Zigbee Network

Mohsen A. M. M. El-Bendary[a], Atef Abou El-Azm[b], Nawal El-Fishawy[b], Farid S. M. Al-Hosarey[b], Mostafa A. R. Eltokhy[a], Fathi E. Abd El-Samie[b], and H. B. Kazemian[c]

[a] *Department of Communication Technology, Faculty of Industrial Education, Helwan University, Egypt*
[b] *Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Egypt*
[c] *Intelligent Systems Research Centre, Faculty of Computing, London Metropolitan University, UK*

Abstract—This paper studies a vital issue in wireless communications, which is the transmission of images over wireless networks. IEEE ZigBee 802.15.4 is a short-range communication standard that could be used for small distance multimedia transmissions. In fact, the ZigBee network is a wireless personal area network (WPAN), which needs a strong interleaving mechanism for protection against error bursts. This paper presents a novel chaotic interleaving scheme for this purpose. This scheme depends on the chaotic Baker map. A comparison study between the proposed chaotic interleaving scheme and the traditional block and convolutional interleaving schemes for image transmission over a correlated fading channel is presented. The simulation results show the superiority of the proposed chaotic interleaving scheme over the traditional schemes.

Keywords—block interleaving, chaotic interleaving, convolutional interleaving, fading channels, ZigBee.

1. Introduction

With the increase in utilization of wireless networks, there are two important factors that deserve consideration; power efficiency and throughput efficiency. Short-range wireless networks such as Bluetooth and ZigBee are widely used for health care and medical applications [1], [2]. The ZigBee network is a low-rate WPAN (LR-WPAN) that is used for short-range and low-cost data communication.

Low power consumption in ZigBee networks can be achieved by allowing a device to sleep, which means waking into active mode for brief periods. Enabling such low duty cycle operation is at the heart of the ZigBee standard [3]. ZigBee is built on top of the IEEE 802.15.4 standard. It offers the additional functionality to implement mesh networking rather than point-to-point networking found in most Bluetooth and Wi-Fi applications. The ZigBee specification document is short, allowing a small and simple stack, in contrast to the other wireless standards such as Bluetooth [4].

The IEEE 802.15.4 standard is intended to conform to established regulations in Europe, Japan, Canada, and the United States. It defines two physical (PHY) layers; the 2.4 GHz and 868/915 MHz band PHY layers. Although the PHY layer chosen depends on local regulations and user preference, only the higher data rate, worldwide, unlicensed 2.4 GHz industrial, scientific and medical frequency band is considered [5]. A total of 16 channels are available in the 2.4 GHz band, numbered from 11 to 26, each with a bandwidth of 2 MHz, and a channel separation of 5 MHz. The channel mapping frequencies are given in Table 1. LR-WPAN output powers are around 0 dBm. LR-WPAN typically operates within a 50-m range. The transmit scheme used is the direct sequence spread spectrum (DSSS) [6].

Table 1
IEEE 802.15.4 frequency bands and data rates

PHY [MHz]	Freq. band [MHz]	Mod.	Channels	Bit rate [kbit/s]
868/915	868-868.6	BPSK	1	20
	902-928	BPSK	10	40
2450	2400-2483.5	O-QPSK	16	250

The ZigBee network involves little or no infrastructure. It also has a primitive error control mechanism, which is the automatic repeat request (ARQ). As a result, this mechanism is unable to reduce the channel effects. So, there is a need for either a coding or interleaving mechanism to combat the bad channel effects [7].

Several papers have studied the transmission of images with the IEEE 802.15.4 standard. In [8], the authors studied the process of image fragmentation for transmission over the ZigBee network. In the case of transmission over mobile networks, there is a probability of burst errors. The burst errors have a bad effect on the transmitted data and image. In this paper, we try to decrease the effect of error bursts on the transmission of images by introducing a powerful chaotic interleaver.

The paper is organized as follows. In Section 2, ZigBee packet format is introduced. In Section 3, the proposed modifications are presented. In Section 4, the simulation assumptions and the simulation results are presented. Finally, the conclusion is presented in Section 5.

2. ZigBee Packet Format

The structure of the ZigBee packet is shown in Fig. 1. The header contains three fields; a preamble of 32 bits for synchronization, a packet delimiter of 8 bits, and a physical header of 8 bits. The physical service data unit (PSDU)

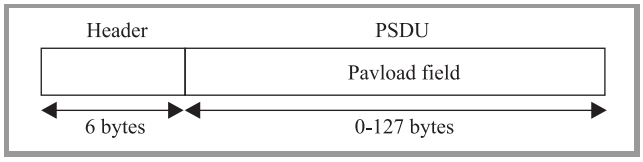


Fig. 1. ZigBee packet format.

field contains a payload of 0 to 127 bytes length. The ZigBee network uses an error detection/retransmission technique. To ensure successful reception of data, an acknowledged frame delivery protocol is supported to increase transfer reliability [9]. The ZigBee network uses the DSSS technique for data transmission, because it increases the immunity to interference. It is based on the multiplication of the original binary stream with a wideband pseudo noise (PN) spreading code, which results in a wideband continuous time scrambled signal. DSSS significantly improves protection against interfering signals, especially narrowband signals. It also provides a multiple access capability, when the several different spreading codes are being used, simultaneously. It also provides a transmission security. DSSS is also used as a technique to generate ultra wide band (UWB) signals [9]. As shown in Fig. 2, the output signal of the modulator $m(t)$ has a much larger bandwidth than the input signal $d(t)$ [10]–[12].

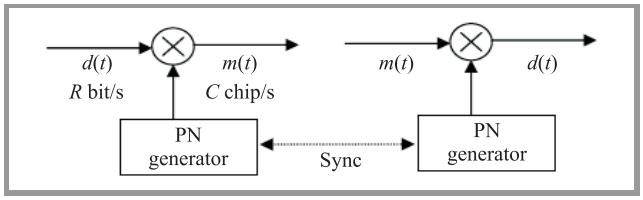


Fig. 2. The direct sequence spread spectrum technique.

Figure 2 shows the stages of the DSSS technique. At the receiver, the wideband signal is despread as shown in the figure. The chip rate C is much larger than the input data rate R.

3. Proposed Modifications

The transmission of multimedia over unreliable data links has become a topic of paramount importance. This type of transmission must reconcile the high data rates involved in multimedia contents and the noisy nature of the channels, be it wireless or mobile. In this paper, we try to improve the transmission of images over the ZigBee network with different interleaving schemes. We study the feasibility of data interleaving prior to transmission over ZigBee networks. The paper presents a new chaotic interleaver and compares it to the traditional block and convolutional interleavers.

3.1. Block Interleaver Scheme

The block interleaving can be used for image transmission with the ZigBee network. After converting the image into a binary sequence, this sequence is rearranged into a matrix in a row-by-row manner, and then read from the matrix in a column-by-column manner. Now take a look at how the block interleaving mechanism can correct error bursts. Assume an error burst affecting four consecutive bits (1-D error burst) as shown in Fig. 3b with shades. After de-interleaving as shown in Fig. 3c, the error burst is effectively spread among four different rows, resulting in a small effect for the 1-D error burst. With a single-error correction capability, it is obvious that no decoding error will result from the presence of such 1-D error burst. This simple example demonstrates the effectiveness of the block interleaving mechanism in combating 1-D error bursts. Let us examine the performance of the block interleaving mechanism, when a 2-D (2×2) error burst occurs [13], as shown in Fig. 3b with shades. Figure 3c indicates that this 2×2 error burst has not been spread, effectively, so that there are adjacent bits in error in the first and second rows. As aeresult, this error burst can not be corrected using a single-error correction mechanism. That is, the block interleaving mechanism can not combat the 2×2 error bursts.

3.2. Convolutional Interleaver Scheme

The convolutional interleaver is constructed by T parallel branches. Each line contains a shift register with a predefined length [14]. The input data is fed into the branches of the interleaver and the output data is taken from the outputs of these branches. In the computer simulations, the length of the interleaver input is 1024 bits, which is the length of the whole payload in ZigBee packets [15].

3.3. Chaotic Interleaver Scheme

As mentioned in the previous subsection, the block interleaver is not efficient with 2-D error bursts. As a result, there is a need for an advanced interleaver for this task. The 2-D chaotic Baker map in its discretized version is a good candidate for this purpose. After rearrangement of bits into a 2-D format, the chaotic Baker map is used to randomize the bits. The discretized Baker map is an efficient tool to randomize the items in a square matrix. Let $B(n_1, \ldots, n_k)$, denote the discretized map, where the vector, $[n_1, \ldots n_k]$, represents the secret key, S_{key}. Defining N as the number of data items in one row, the secret key is chosen such that each integer n_i divides N, and $n_1 + \ldots, +n_k = N$.
Let $N_i = n_1 + \ldots, +n_{i-1}$. The data item at the indices (r, s), is moved to the indices [16]–[20]:

$$B(r,s) = \left[\frac{N}{n_i}(r - N_i) + s \bmod \left(\frac{N}{n_i}\right),\ \frac{n_i}{N}\left(s - s \bmod \left(\frac{N}{n_i}\right)\right) + N_i\right], \tag{1}$$

where $N_i \le r < N_i + n_i$, $0 \le S < N$, and $N_1 = 0$.

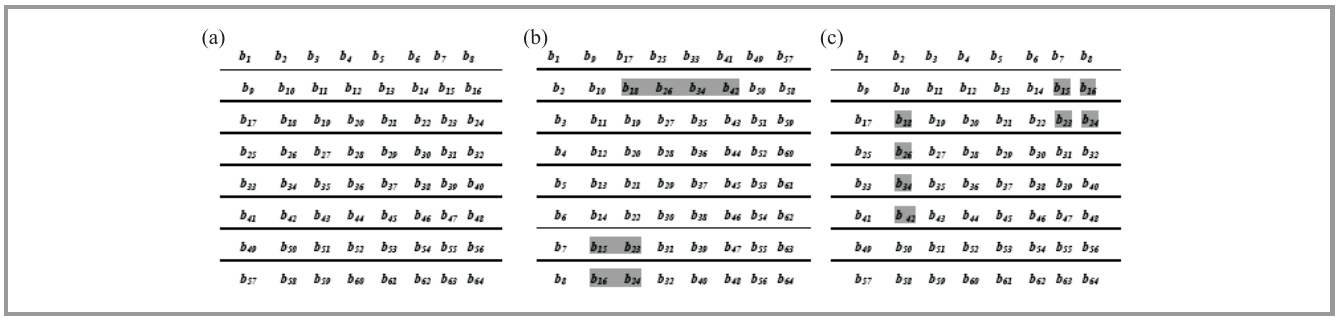


Fig. 3. Block interleaving of an 8×8 matrix: (a) the 8×8 matrix, (b) block interleaving of the matrix, (c) effect of error bursts after de-interleaving.

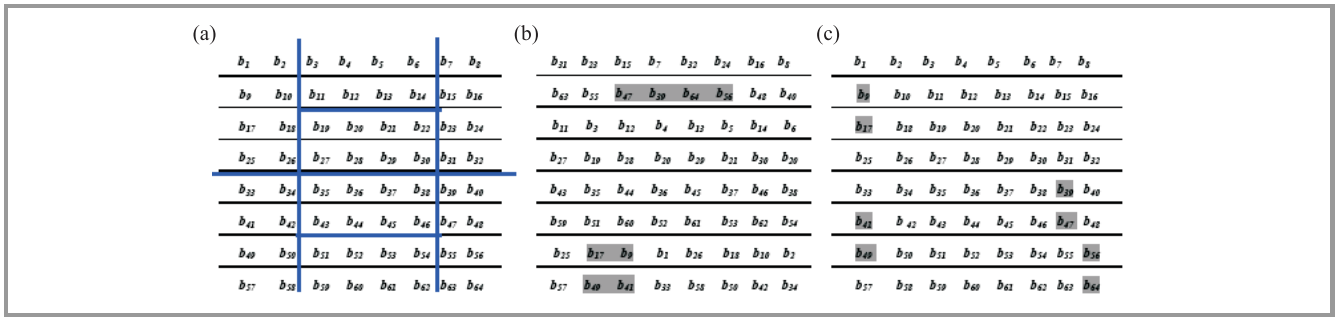


Fig. 4. Chaotic interleaving of an 8×8 matrix: (a) the 8×8 matrix divided into rectangles (shaded bits are bits affected by error bursts), (b) chaotic interleaving of the matrix, (c) effect of error bursts after de-interleaving.

In steps, the chaotic permutation is performed as follows:

1. An $N \times N$ square matrix is divided into N rectangles of width n_i and number of elements N.
2. The elements in each rectangle are rearranged to a row in the permuted rectangle. Rectangles are taken from left to right beginning with upper rectangles then lower ones.
3. Inside each rectangle, the scan begins from the bottom left corner towards upper elements.

Figure 4 shows an example for chaotic interleaving of an 8×8 square matrix (i.e., $N = 8$). The secret key, $S_{key} = [n_1, n_2, n_3] = [2, 4, 2]$. Note that, the chaotic interleaving mechanism has a better treatment to both 1-D and 2-D error bursts than the block interleaving mechanism. Errors are better distributed to bits after de-interleaving in the proposed chaotic interleaving scheme. As a result, a better peak signal to noise ratio (PSNR) of received images can be achieved with this proposed mechanism. Moreover, it adds a degree of security to the communication system. At the receiver of the ZigBee system, a chaotic de-interleaving step is performed.

4. Simulation Results

In this section, the computer simulation results are presented. An important assumption used in the simulation is that a packet is discarded if there is an error in either the header or the payload field [21]. This is a realistic assumption to simulate the real ZigBee system operation. A correlated Rayleigh fading channel is used. The channel model utilized is the Jake's model [22]–[23]. The assumed mobile ZigBee device velocity is 10 miles/hour, and the carrier frequency is 2.46 GHz. The Doppler spread is 36.6 Hz. Figure 5 gives the original cameraman image used in the experiments. It is the Matlab image and it format is tag image file format (TIF).

Fig. 5. Original cameraman image.

The image binary sequence to be transmitted is fragmented into packets. The PSNR of the received images is used as an evaluation metric in this paper.

In the first computer simulation, the cameraman image is transmitted over a correlated fading channel with signal to

noise ratio (SNR) = 10 dB. Three scenarios of no interleaving, block interleaving, convolutional interleaving and chaotic interleaving are considered for comparison. The results of this experiment are shown in Fig. 6. From these results, it is clear that the effect of all interleaving schemes is approximately equal at low SNR values.

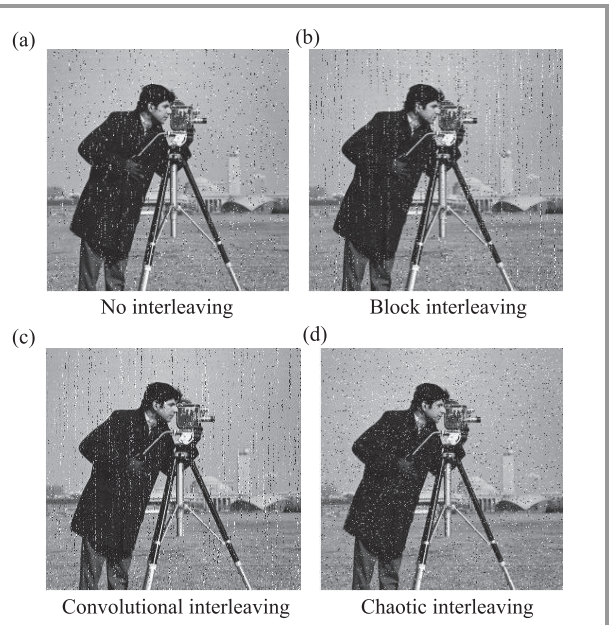


Fig. 6. Received cameraman image over a correlated fading channel at SNR = 10 dB with (a) PSNR = 21.3 dB, (b) PSNR = 21.4 dB, (c) PSNR = 21.1 dB, and (d) PSNR = 21.5 dB.

Other experiments are repeated with SNR = 20 and 30 dB and the results are shown in Figs. 7 and 8, respectively.

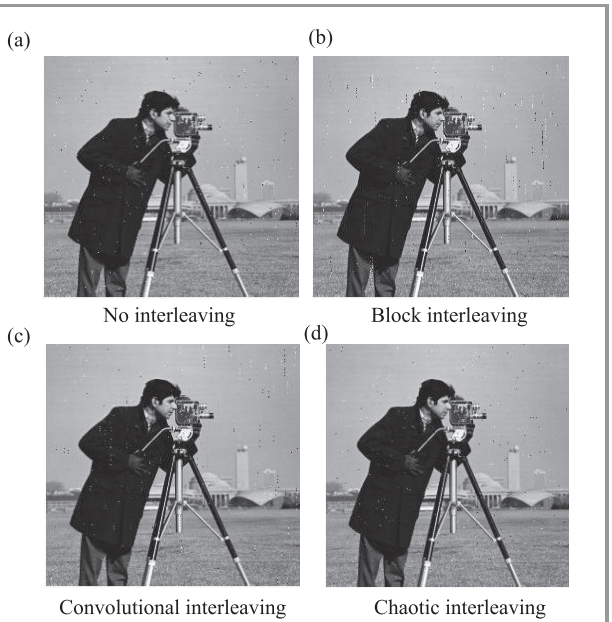


Fig. 7. Received cameraman image over a correlated fading channel at SNR = 20 dB with (a) PSNR = 31.1 dB, (b) PSNR = 31.5 dB, (c) PSNR = 32.1 dB, and (d) PSNR = 33.2 dB.

From these results, we notice that the chaotic interleaver outperforms the other interleavers at moderate to high SNRs.

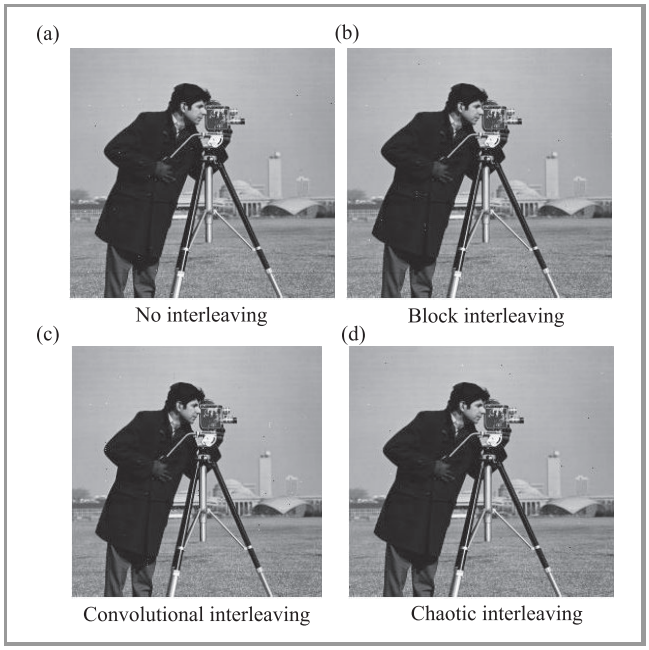


Fig. 8. Received cameraman image over a correlated fading channel at SNR = 30 dB with (a) PSNR = 39.1 dB, (b) PSNR = 41 dB, (c) PSNR = 41.1 dB, and (d) PSNR = 43.1 dB.

For the comparison purpose, the variation of the PSNR of the received image, the number of lost frames and the bit error rate (BER) with the channel SNR are studied and the results are shown in Figs. 9–11. From these results, it is clear the chaotic interleaver enhancement begins at medium SNR values.

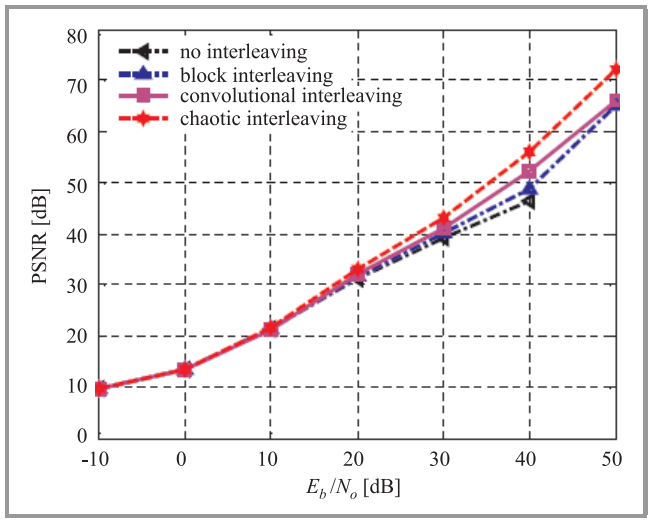


Fig. 9. PSNR versus SNR for the received cameraman image over a correlated fading channel.

As shown in these figures, the proposed chaotic interleaver does not decrease the number of lost frames, but it enhances the PSNR of the received images at medium to high SNR

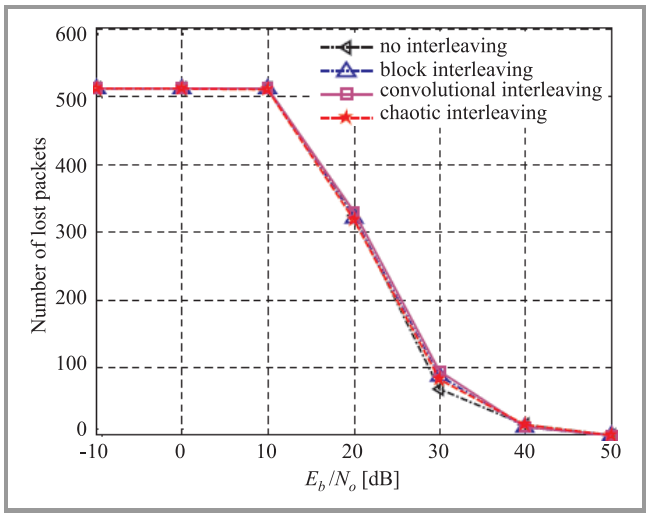


Fig. 10. Number of lost frames versus SNR for the received cameraman image over a correlated fading channel.

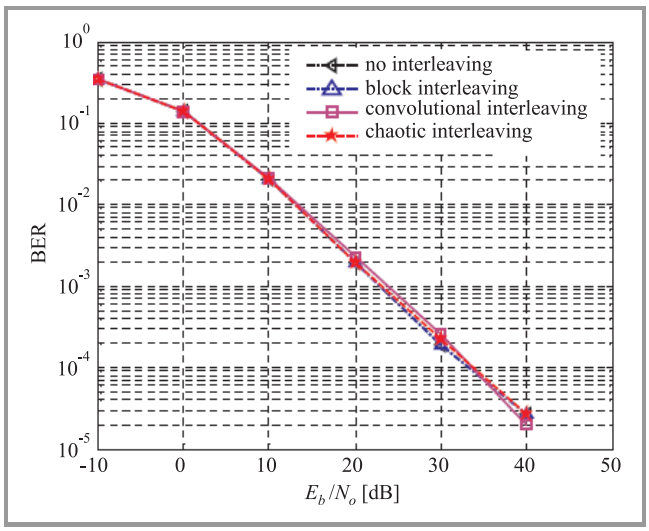


Fig. 11. BER versus SNR for the received cameraman image over a correlated fading channel.

values. The powerful of the proposed technique due to the ZigBee standard doesn't employ error control codes scheme with the transmitted packets. So, there is the possibility using of the chaotic interleaver over the mobile ZigBee network for improve the received image quality with the security enhancing.

5. Conclusion

This paper presented a simple and efficient novel chaotic interleaver for the transmission of images over the ZigBee network. A comparison study between the proposed interleaver and the conventional interleavers has been presented. The computer simulation results have revealed the effectiveness of the proposed interleaver at medium and high SNR values. Also, the proposed interleaver enhanced the security level over the ZigBee network link, as it is based on chaotic map encryption.

References

[1] "ZigBee Alliance", 2009 [Online]. Available: http://www.zigbee.org/

[2] "The Wi-Fi Alliance", 2009 [Online]. Available: http://www.wi-fi.org/

[3] B. Kai and P. Yong, "Performance study on ZigBee-based wireless personal area networks for real-time health monitoring", *ETRI J.*, vol. 28, no. 4, 2006.

[4] J.-S. Lee, Y.-W. Su, and C.-C. Shen," A comparative study of wireless protocols: Bluetooth, UWB, ZigBee, and Wi-Fi", in *Proc. 33rd Ann. Conf. IEEE Industr. Electron. Soc. IECON*, Taipei, Taiwan, 2007.

[5] W. Guo and M. Zhou,"An emerging technology for improved building automation control", in *Proc. IEEE Int. Conf. Syst. Man Cybern. IEEE SMC 2009*, San Antonio, USA, 2009, pp. 337–342.

[6] B. Sidhu, H. Singh, and A. Chhabra,"Emerging wireless standards – WiFi, ZigBee and WiMAX s", in *World Academy of Science, Engineering and Technology*, vol. 25, 2007.

[7] S. Vafi and T. Wysocki,"Performance of convolutional interleavers with different spacing parameters in turbo codes", in *Proc. 6th Australian Commun. Theory Worksh.*, Brisbane, Australia, 2005, pp. 8–12.

[8] G. Pekhteryev, Z. Sahinoglu, P. Orlik, and G. Bhatti, "Image transmission over IEEE 802.15.4 and ZigBee networks", in *Proc. IEEE ISCAS*, Kobe, Japan, 2005.

[9] L. Ozarow, S. Shamai, and A.D. Wyner,"Information theoretic considerations for cellar mobile radio", *IEEE Trans. Veh. Technol.*, vol. 43, pp. 359–378, 1994.

[10] E. N. Farag and M. I. Elmasry, *Mixed Signal VLSI Wireless Design Circuits and System*. Kluwer, 1999.

[11] [11] H. S. Kim and H. K. Lee, "Modified beacon-enabled IEEE 802.15.4 MAC for lower latency", *Mitsubishi Electric Research Laboratories*, 201 Broadway, Cmbridge, Massachusetts 02139, 2009.

[12] T. S. Rappaport, *Wireless Communications*. Prentice Hall, 1996.

[13] S. H. Lee and E. K. Joo, , "The effect of block interleaving in an LDPC-turbo concatenated code", *ETRI J.*, vol. 28, no. 5, 2006.

[14] S. Vafi and T. A. Wysocki, "Application of convolutional interleavers in turbo codes with unequal error protection", *J. Telecommun. Inform. Technol.*, no. 1, pp. 17–23, 2006.

[15] G. Pekhteryev, Z. Sahinoglu, P. Orlik, and G. Bhatti, "Error protection for progressive image transmission over memoryless and fading channels", *IEEE Transactions on Communications*, vol. 46, no. 12, Dec. 1998.

[16] A. N. Lemma, J. Aprea, W. Oomen, and L. V. de Kerkhof, "A temporal domain audio watermarking technique", *IEEE Trans. Sig. Process.*, vol. 51, no. 4, pp. 1088–1097, 2003.

[17] W. Li, X. Xue, and P. Lu, "Localized audio watermarking technique robust against time-scale modification", *IEEE Trans. Multim.*, vol. 8, no. 1, pp. 60–69, 2006.

[18] G. Voyatzis and I. Pitas,"Chaotic watermarks for embedding in the spatial digital image domain", in *Proc. IEEE Int. Conf. Image Process.*, vol. 2, pp. 432–436, Oct. 1998.

[19] R. Liu and T. Tan, "An SVD-based watermarking scheme for protecting rightful ownership", *IEEE Trans. Multim.*, vol. 4, no. 1, pp. 121–128, 2002.

[20] Z. Liu and A. Inoue, "Audio watermarking techniques using sinusoidal patterns based on pseudorandom sequences", *IEEE Trans. Circ. Sys. Video Technol.*, vol. 13, no. 8, pp. 801–812, 2003.

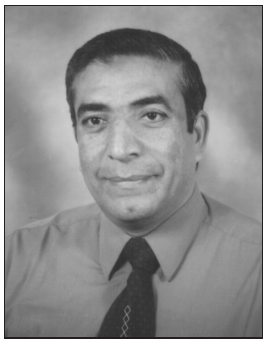
[21] M. A. M. Mohamed, A. Abou El-Azm, N. El-Fishwy, M. A. R. El-Tokhy, and F. E. Abd El-Samie,"Optimization of Bluetooth packet format for efficient performance", *Progress in Electromagn. Res. M*, vol. 1, pp. 101–110, 2008.

[22] W. C. Jakes, *Microwave Mobile Communications*. New York: Wiley, 1975.

[23] J. Aldrich,"Correlations genuine and spurious in Pearson and Yule", *Statistical Science*, vol. 10, no. 4, pp. 364-376, 1996 [Online]. Available: hppt://www.jstor.org/stable/2246135

Mohsen A. M. Mohamed El-Bendary received his B.Sc. in 1998, M.Sc. in 2008, all in communication engineering, from Menoufia University, Faculty of electronic Engineering. He is now a lecturer assistant and Ph.D. student. His research interests cover wireless networks, wireless technology, channel coding, QoS over Bluetooth system and Wireless Sensor Network (WSN), and security systems which use wireless technology, such as fire alarm and access control systems.

e-mail: mohsenbendary@yahoo.com
Faculty of Industrial Education
Department of Communication Technology
Helwan University, Egypt



Atef Abou El-Azm was born in 1954, Egypt. He has the B.Sc. in electronic engineering and M.Sc. in antennas from Faculty of Electronic Engineering, Menofia University in 1977 and 1984, respectively. He has the Ph.D. in communications from Warsaw University of Technology, Poland, in 1990. His research is in the area of digital communications, with special emphasis on coding theory, information theory, error control coding, and coded modulation. Topics of current interest include the use of convolutional, trellis codes and turbo codes in the development of coding standards for high speed data modems, digital satellite communication, and deep space channels. He is the author of many papers in the field of line codes, channel codes and signal processing.

e-mail: abouelazm_atef@yahoo.com
Faculty of Electronic Engineering
Department of Electronics and Electrical Communications
Menoufia University
Menouf, 32952, Egypt

Nawal El-Fishawy received the Ph.D. degree in mobile communications from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in collaboration with Southampton University in 1991. Now she is the head of Computer Science and Engineering Department, Faculty of Electronic Eng. Her research interest includes computer communication networks with emphasis on protocol design, traffic modeling and performance evaluation of broadband networks and multiple access control protocols for wireless communications systems and networks. Now she directed her research interests to the developments of security over wireless communications networks (mobile communications, WLAN, Bluetooth), VOIP, and encryption algorithms.

e-mail: nelfishawy@hotmail.com
Faculty of Electronic Engineering
Department of Electronics and Electrical Communications
Menoufia University
Menouf, 32952, Egypt

Farid Shawki M. Al-Hosarey received the B.Sc. (Hons), M.Sc., and Ph.D. degrees from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1995, 2000 and 2007, respectively. In 1995 and 2000, he worked as a demonstrator and assistant lecturer in the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering respectively. He joined the teaching staff of the Department of Electronics and Electrical Communications since 2008. His current research areas of interest include Channel Coding, Mobile communication Systems, MIMO systems, and Implementation of Digital communications Systems using FPGA.

e-mail: farid_shawki@yahoo.com
Faculty of Electronic Engineering
Department of Electronics and Electrical Communications
Menoufia University
Menouf, 32952, Egypt

Mostafa A. R. Eltokhy was born in Kaluobia, Egypt, in 1970. He received his B.Sc. degree from Zagazig University, Banha branch, Egypt, and M.Sc. degree from Technical University, Eindhoven, The Netherlands in 1993 and 1998, respectively. He received his Ph.D. degree from Osaka University, Osaka, Japan in 2003. Presently, he is an Assistant Professor of Electronics Engineering at Industrial Education College, Higher ministry of Education, Cairo Egypt. His current research interests are high performance digital circuits and analog circuits. He is a member of the IEEE.

e-mail: mostafaeltokhy@hotmail.com
Faculty of Industrial Education
Department of Communication Technology
Helwan University, Egypt

Fathi E. Abd El-Samie received the B.Sc. (Honors), M.Sc., and Ph.D. from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. He joined the teaching staff of the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2005. He is a co-author of about 130 papers in national and international conference proceedings and journals. He has received the most cited paper award from Digital Signal Processing journal for 2008. His current research areas of interest include image enhancement, image restoration, image interpolation, superresolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications.
e-mail: fathi_sayed@yahoo.com
Faculty of Electronic Engineering
Department of Electronics and Electrical Communications
Menoufia University
Menouf, 32952, Egypt

H. B. Kazemian (SM'1988) received the B.Sc. in engineering from Oxford Brookes University, UK, the M.Sc. in control systems engineering from the University of East London, UK, and the Ph.D. in learning fuzzy controllers from Queen Mary University of London, UK, in 1985, 1987 and 1998, respectively. He is currently a Full Professor at London Metropolitan University, UK. He worked for Ravensbourne College University Sector, UK, as a senior lecturer for eight years. Previous lecturing experience includes the University of East London, University of Northampton, and Newham College. Research interests include fuzzy and neuro-fuzzy control of networks, 2.4 GHz frequency bands (ZigBee, Bluetooth, WiFi), ATM, video streaming and rate control. He is a senior member of the Institute of Electrical and Electronics Engineers (SMIEEE), Fellow of the Institution of Engineering and Technology FIET (formerly IEE), and Chartered Engineer, UK.
e-mail: h.kazemian@londonmet.ac.uk
Intelligent Systems Research Centre
Faculty of Computing
London Metropolitan University
London, UK

Paper

Higher Order Cumulants for Identification and Equalization of Multicarrier Spreading Spectrum Systems

Said Safi[a], Miloud Frikel[b], Abdelouhab Zeroual[c], and Mohammed M'Saad[b]

[a]Polydisciplinary Faculty, Sultan Moulay Slimane University, Morocco
[b] GREYC, Ecole Nationale Supérieure d'Ingénieurs de Caen, France
[c]Department of Physics, Faculty of Sciences Semlalia, Cadi Ayyad University, Morocco

Abstract—This paper describes two blind algorithms for multicarrier code division multiple access (MC-CDMA) system equalization. In order to identify, blindly, the impulse response of two practical selective frequency fading channels called broadband radio access network (BRAN A and BRAN E) normalized for MC-CDMA systems, we have used higher order cumulants (HOC) to build our algorithms. For that, we have focussed on the experimental channels to develop our blind algorithms able to simulate the measured data with high accuracy. The simulation results in noisy environment and for different signal to noise ratio (SNR) demonstrate that the proposed algorithms are able to estimate the impulse response of these channels blindly (i.e., without any information about the input), except that the input excitation is i.i.d. (identically and independent distributed) and non-Gaussian. In the part of MC-CDMA, we use the zero forcing and the minimum mean square error equalizers to perform our algorithms. The simulation results demonstrate the effectiveness of the proposed algorithms.

Keywords—blind identification and equalization, communication channels, higher order cumulants, MC-CDMA systems.

1. Introduction

Many important results [1]–[8] are established that blind identification of finite impulse response (FIR) single-input single-output (SISO) communication channels is possible only from the output second-order statistics, without using any restrictive assumption on the channel zeros, color of additive noise, channel order over-estimation errors, and without increasing the transmission rate of the data stream. Those algorithms have been termed transmitter-induced multistationary approaches. Some class of algorithms for blind channel identification are based on the iterative strategy.

The interest in higher order cumulants (HOC) or higher order statistics (HOS) is permanently growing in the last years. Principally finite impulse response system identification based on HOC of system output has received more attention. Tools that deal with problems related to either nonlinearity, non-Gaussianity, or non-minimum phase (NMP) systems are available, because they contain the phase information of the underlying linear system in contrast to second order statistics, and they are of great value in applications, such as radar, sonar, array processing, blind equalization, time delay estimation, data communication, image and speech processing and seismology [9]–[12].

Many algorithms have been proposed in the literature for the identification of FIR system using cumulants. These algorithms can be classified into three broad classes of solutions: closed form solutions [13], [14], [15], optimization based solutions [16], [17] and linear algebra solutions [18]–[25]. The linear algebra solutions have received great attention because they have "simpler" computation and are free of the problems of local extreme values that often occur in the optimization solution. Although, the closed-form solutions have similar features, they usually do not smooth out the noises caused from the observation and computation. Therefore, while these solutions are interesting from the theoretical point of view, they are not recommended for practical applications [26], [25]. The main goal of this investigation is to elaborate an accurate and efficient algorithm able to estimate the moving average (MA) (or FIR) parameters in noisy environment. So, we address the problem of estimating the parameters of a FIR system from the output observation when the system is excited by an unobservable independent identically distributed (i.i.d.) sequence. The proposed algorithms, based on third and fourth order cumulants, to estimate the parameters of MA process when the order is known, are presented. For validation purpose these method are used to search for a model able to describe the broadband radio access network (BRAN A and BRAN E) channels, represented by a FIR model.

In this paper we present two algorithms based on linear algebra solutions. These algorithms are based on third and fourth order cumulants. Our goal in this paper is to find a model able to represent the mobile channels without reference to the measures, standardized by the European Telecommunications Standards Institute (ETSI) for the "inside" indoor (BRAN A) or "outside" of an outdoor office (BRAN E) [27], [28]. Similarly, we perform the equal-

ization, using the model developed a multicarrier multiple access division of codes (MC-CDMA) downlink [29], [30]. For this, we develop a "blind" algorithm able to simulate the measured data with high accuracy in noisy environment, and for different signal to noise ratio (SNR).

So, we have, principally, focussed on channel impulse response estimation. The considered channels are with non-minimum phase and selective frequency (i.e., normalized channels for MC-CDMA: BRAN A, BRAN E). In most wireless environments, there are many obstacles in the channels, such as buildings, mountains and walls between the transmitter and the receiver. Reflections from these obstacles cause many different propagation paths. This is called multipaths propagation or a multipath channel. The frequency impulse response of this channel, is not flat (ideal case) but comprising some hollows and bumps, due to the echoes and reflection between the transmitter and the receiver. Another problem encountered in communication is the synchronization between the transmitter and the receiver. To solve the problem of phase estimation we will use higher order cumulants (HOC) to test the robustness of those techniques if the channel is affected by noise. HOC are a fairly topic with many applications in system theory. The HOC are only applicable to non-Gaussian and non-linear process because the cumulants of a Gaussian process are identically zero [2], [21], [31]. Many real world applications are truly non-Gaussian [2], [4], [32]. Also, the Fourier transformation of HOC, which is termed higher order spectra (or polyspectra), provides an efficient tool for solving the problem of equalization technology used in communication. The major feature of HOC, from the point of view of equalization, is that the phase information of channels is present [7], [22], [23], [33]. Therefore they can be used to estimate the parameters of the channel model without any knowledge of the phase property (minimum phase – MP or non-minimum phase – NMP) of channel or the transmitted data (assuming a non-Gaussian distribution) [2], [4], [26].

In this paper, we propose two algorithms based on third and forth order cumulants. In order to test its efficiency, we have considered practical, i.e., measured, frequency-selective fading channel, called broadband radio access network, representing respectively the transmission in indoor and outdoor scenarios. These model radio channels are normalized by the ETSI in [27], [28]. Post-equalization at the receiver for downlink MC-CDMA systems in the form of single-user detection (SUD), i.e., transmission from the base station to the mobile systems, has been investigated by several authors, [34], [32], [35]. Recently, pre-equalization at the transmitter for downlink time division duplex (TDD), MC-CDMA has attained increased interest and has been investigated in details [30], [32], [34], [36], [37]. In this contribution, the novel concept of blind equalization is developed and investigated for downlink MC-CDMA systems. This paper shows that we can identify and equalize the MC-CDMA systems blindly. However, the classical equalization of MC-CDMA system assumes that the channel is known. The bit error rate (BER) performances of the downlink MC-CDMA systems, using blind BRAN A and BRAN E estimation, are shown and compared with the results obtained with the classical methods (in which, the channel parameters are assumed known).

1.1. Problem Statement

The output of a FIR channel, excited by an unobservable input sequences, i.i.d. zero-mean symbols with unit energy, across a selective channel with memory p and additive noise (Figure 1). The output time series is described by the following equation

$$r(k) = h_p x(k) + n(k), \tag{1}$$

where $h_p = (h(1), h(2), \ldots, h(p))$ represents the channel impulse response, $x(k)$ and $n(t)$ is the additive colored Gaussian noise with energy $E\{n^2(k)\} = \sigma^2$.

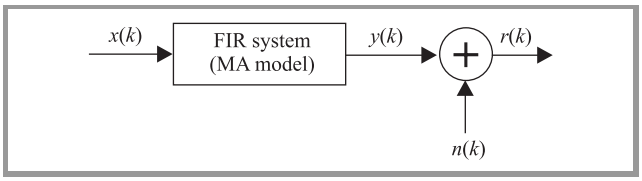


Fig. 1. Channel model.

The completely blind channel identification problem is to estimate h_p based only on the received signal $r(k)$ and without any knowledge of the energy of the transmitted data $x(k)$ nor the energy of noise.
The output of the channel is characterized by its impulse response $h(n)$, which we identify "blindly" its parameters, is given by the following equation

$$y(k) = \sum_{i=0}^{P} x(i)h(k-i); \quad r(k) = y(k) + n(k). \tag{2}$$

1.2. Proposed Algorithms

1.2.1. Algorithm Based on 3th Order Cumulant: Alg. 1

Hypothesis:

Let us suppose that:

- The additive noise $n(k)$ is Gaussian, colored or with symmetric distribution, zero mean, with variance σ^2, i.i.d. with the m^{th} order cumulants vanishes for $m > 2$.
- The noise $n(t)$ is independent of $x(k)$ and $y(k)$.
- The channel (FIR system) order p is supposed to be known and $h(0) = 1$.
- The system is causal, i.e., $h(i) = 0$ if $i < 0$.

The mth order cumulant of the output signal is given by the following equation [21], [38], [39]:

$$C_{my}(t_1,...,t_{m-1}) = \gamma_{mx} \sum_{i=-\infty}^{+\infty} h(i)h(i+t_1)...h(i+t_{m-1}), \quad (3)$$

where γ_{mx} represents the m^{th} order cumulants of the excitation signal $(x(k))$ at origin.
If $m = 3$, Eq. (3) yield to

$$C_{3y}(t_1,t_2) = \gamma_{3x} \sum_{i=0}^{P} h(i)h(i+t_1)h(i+t_2), \quad (4)$$

the same, if $m = 2$, Eq. (3) becomes

$$C_{2y}(t_1) = \sigma^2 \sum_{i=0}^{P} h(i)h(i+t_1). \quad (5)$$

The Fourier transform of Eqs. (4) and (5) gives us the bispectra and the spectrum respectively

$$S_{3y}(\omega_1,\omega_2) = \gamma_{3x} H(\omega_1)H(\omega_2)H(-\omega_1-\omega_2), \quad (6)$$

$$S_{2y}(\omega) = \sigma^2 H(\omega)H(-\omega). \quad (7)$$

If we suppose that $\omega = (\omega_1+\omega_2)$, Eq. (7) becomes

$$S_{2y}(\omega_1+\omega_2) = \sigma^2 H(\omega_1+\omega_2)H(-\omega_1-\omega_2), \quad (8)$$

then, from Eqs. (6) and (8) we obtain the following equation

$$H(\omega_1+\omega_2)S_{3y}(\omega_1+\omega_2) = \varepsilon H(\omega_1)H(\omega_2)S_{2y}(\omega_1+\omega_2), \quad (9)$$

where $\varepsilon = (\frac{\gamma_{3x}}{\sigma^2})$.
The inverse Fourier transform of Eq. (9) demonstrates that the 3rd order cumulants, the auto-correlation function (ACF) and the impulse response channel parameters are combined by the following equation

$$\sum_{i=0}^{P} h(i)C_{3y}(t_1-i,t_2-i) = \varepsilon \sum_{i=0}^{P} h(i)h(i+t_2-t_1)C_{2y}(t_1-i). \quad (10)$$

If we use the property of the ACF of the stationary process, such as $C_{2y}(t) \neq 0$ only for $(-p \leq t \leq p)$ and vanishes elsewhere. In addition, if we take $t_1 = -p$, Eq. (10) takes the form

$$\sum_{i=0}^{P} h(i)C_{3y}(-p-i,t_2-i) = \varepsilon h(0)h(t_2+p)C_{2y}(-p), \quad (11)$$

else, if we suppose that $t_2 = -p$, Eq. (11) will become

$$C_{3y}(-p,-p) = \varepsilon h(0)C_{2y}(-p). \quad (12)$$

Using Eqs. (11) and (12) we obtain the following relation

$$\sum_{i=0}^{P} h(i)C_{3y}(-p-i,t_2-i) = h(t_2+p), \quad (13)$$

else, if we suppose that the system is causal, i.e., $h(i) = 0$ if $i < 0$. So, for $t_2 = -p,...,0$, the system of Eq. (13) can be written in matrix form as

$$\begin{pmatrix} C_{3y}(-p-1,-p-1) & \dots & C_{3y}(-2p,-2p) \\ C_{3y}(-p-1,-p)-\alpha & \dots & C_{3y}(-2p,-2p+1) \\ \vdots & \ddots & \vdots \\ C_{3y}(-p-1,1) & \dots & C_{3y}(-2p,-p)-\alpha \end{pmatrix} \begin{pmatrix} h(1) \\ h(2) \\ \vdots \\ h(p) \end{pmatrix} = \begin{pmatrix} 0 \\ -C_{3y}(-p,-p+1) \\ \vdots \\ -C_{3y}(-p,0) \end{pmatrix}, \quad (14)$$

where $\alpha = C_{3y}(-p,-p)$.
The above Eq. (14) can be written in compact form as

$$Mh_p = d_1, \quad (15)$$

where M is the matrix of size $(p+1)\times(p)$ elements, h_p is a column vector constituted by the unknown impulse response parameters $h(n) : n = 1,\dots,p$ and d is a column vector of size $(p+1)\times(1)$ as indicated in the Eq. (14). The least squares solution (LS) of the system of Eq. (15), permits blindly identification of the parameters $h(n)$ and without any "information" of the input selective channel. So, the solution will be written under the following form

$$h_p = (M^T M)^{-1} M^T d_1. \quad (16)$$

1.2.2. Algorithm Based on 4^{th} Order Cumulants: Alg. 2

From the Eq. (3), the m^{th} and n^{th} cumulants of the output signal, $\{y(n)\}$, and the coefficients $\{h(i)\}$, where $n > m$, are linked by the following relationship:

$$\sum_{j=0}^{p} h(j)C_{ny}(j+t_1,\dots,j+t_{m-1},t_m,\dots,t_{n-1}) = \frac{\gamma_{ne}}{\gamma_{me}} \sum_{i=0}^{p} h(i) \left[\prod_{k=m}^{n-1} h(i+t_k)\right] C_{my}(i+t_1,\dots,i+t_{m-1}). \quad (17)$$

If we take $n = 4$ and $m = 3$ into Eq. (17), we find the basic relationship developed in [40], [41]. If we take $n = 3$ and $m = 2$ into Eq. (16), we find the basic relationship of the algorithms developed in [2].
So, the equation proposed in [42] presents the relationship between different n^{th} cumulant slices of the output signal $\{y(n)\}$, as follows

$$\sum_{j=0}^{p} h(j) \left[\prod_{k=1}^{r} h(j+t_k)\right] C_{ny}(\beta_1,\dots,\beta_r,j+\alpha_1,\dots,\alpha_{n-r-1}) = \sum_{i=0}^{p} h(i) \left[\prod_{k=1}^{r} h(i+\beta_k)\right] C_{ny}(t_1,\dots,t_r,i+\alpha_1,\dots,i+\alpha_{n-r-1}), \quad (18)$$

where $1 \leq r \leq n-2$.

If we take $n=3$ we obtain that $r=1$, so the Eq. (17) will be

$$\sum_{j=0}^{p} h(j)h(j+t_1)C_{3y}(\beta_1, j+\alpha_1) = \sum_{i=0}^{p} h(i)h(i+\beta_1)C_{3y}(t_1, i+\alpha_1). \tag{19}$$

In the following, we develop an algorithm based only on 4^{th} order cumulants.

If we take $n=4$ into Eq. (18) we obtain the following equation:

$$\begin{aligned} &\sum_{i=0}^{p} h(i)h(i+t_1)h(i+t_2)C_{4y}(\beta_1,\beta_2,i+\alpha_1) \\ &= \sum_{j=0}^{p} h(j)h(j+\beta_1)h(j+\beta_2)C_{4y}(t_1,t_2,j+\alpha_1), \end{aligned} \tag{20}$$

if $t_1=t_2=p$ and $\beta_1=\beta_2=0$, Eq. (20) take the form:

$$h(0)h^2(p)C_{4y}(0,0,i+\alpha_1) = \sum_{j=0}^{p} h^3(j)C_{4y}(p,p,j+\alpha_1). \tag{21}$$

As the system is a FIR, and is supposed causal with an order p, so, the $j+\alpha_1$ will be necessarily into the interval $[0,p]$, this implies that the determination of the range of the parameter $\alpha_1$is obtained as follows: $0 \le j+\alpha_1 \le p \Rightarrow -j \le \alpha_1 \le q-j$, and we have $0 \le j \le p$. From these two inequations, we obtain:

$$-p \le \alpha_1 \le p. \tag{22}$$

Then, from the Eqs. (20) and (21) we obtain the following system of equations :

$$\begin{pmatrix} C_{4y}(p,p,-p) & \cdots & C_{4y}(p,p,0) \\ \vdots & \ddots & \vdots \\ C_{4y}(p,p,0) & \cdots & C_{4y}(p,p,p) \\ \vdots & \ddots & \vdots \\ C_{4y}(p,p,p) & \cdots & C_{4y}(p,p,2p) \end{pmatrix} \begin{pmatrix} h^3(0) \\ \vdots \\ h^3(i) \\ \vdots \\ h^3(p) \end{pmatrix} = h(0)h^2(p) \begin{pmatrix} C_{4y}(0,0,-p) \\ \vdots \\ C_{4y}(0,0,0) \\ \vdots \\ C_{4y}(0,0,p) \end{pmatrix} \tag{23}$$

and as we have assumed that $h(0)=1$, if, we consider that $h(p)\neq 0$ and the cumulant $C_{my}(t_1,\ldots,t_{m-1})=0$, if one of the variables $t_k > p$, where $k=1,\ldots,m-1$; the system of Eq. (23) will be written as follows:

$$\begin{pmatrix} 0 & \cdots & 0 & C_{4y}(p,p,0) \\ \vdots & \ddots & & \vdots \\ 0 & & & \\ C_{4y}(p,p,0) & \cdots & & C_{4y}(p,p,p) \\ \vdots & \ddots & & 0 \\ & & & \vdots \\ C_{4y}(p,p,p) & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} \frac{1}{h^2(p)} \\ \vdots \\ \frac{h^3(i)}{h^2(p)} \\ \vdots \\ \frac{h^3(p)}{h^2(p)} \end{pmatrix} = \begin{pmatrix} C_{4y}(0,0,-p) \\ \vdots \\ C_{4y}(0,0,0) \\ \vdots \\ C_{4y}(0,0,p) \end{pmatrix}. \tag{24}$$

In more compact form, the system of Eq. (24) can be written in the following form:

$$Mb_{p_2} = d_2, \tag{25}$$

where M, b_q and d are defined in the system of Eq. 24). The least squares solution of the system of Eq. (25) is given by:

$$\hat{b}_{p_2} = (M^T M)^{-1} M^T d_2. \tag{26}$$

This solution give us an estimation of the quotient of the parameters $h^3(i)$ and $h^3(p)$, i.e., $b_{p_2}(i) = \widehat{\left(\frac{h^3(i)}{h^3(p)}\right)}$, $i=1,\ldots,p$. So, in order to obtain an estimation of the parameters $\hat{h}(i)$, $i=1,\ldots,p$ we proceed as follows:

- The parameters $h(i)$ for $i=1,\ldots,p-1$ are estimated from the estimated values $\hat{b}_p(i)$ using the following equation:

$$\hat{h}(i) = \text{sign}\left[\widehat{b}_{p_2}(i)(\widehat{b}_{p_2}(p))^2\right]\left\{\text{abs}(\hat{b}_{p_2}(i))(\hat{b}_{p_2}(p))^2\right\}^{\frac{1}{3}} \tag{27}$$

  where $\text{sign}(x) = \begin{cases} 1, & \text{if } x>0; \\ 0, & \text{if } x=0; \\ -1, & \text{if } x<0. \end{cases}$

  and $\text{abs}(x)=|x|$ indicates the absolute value of x.

- The $\hat{h}(p)$ parameters is estimated as follows :

$$\hat{h}(p) = \frac{1}{2}\text{sign}\left[\hat{b}_{p_2}(p)\right]\left\{\text{abs}(\hat{b}_{p_2}(p)) + \left(\frac{1}{\hat{b}_{p_2}(1)}\right)^{\frac{1}{2}}\right\}. \tag{28}$$

2. Application: Identification and Equalization of MC-CDMA System

The principles of MC-CDMA [37] is that a single data symbol is transmitted at multiple narrow band subcarriers. Indeed, in MC-CDMA systems, spreading codes are

applied in the frequency domain and transmitted over independent sub-carriers. However, multicarrier systems are very sensitive to synchronization errors such as symbol timing error, carrier frequency offset and phase noise. Synchronization errors cause loss of orthogonality among subcarriers and considerably degrade the performance especially when large number of subcarriers presents. There have been many approaches on synchronization algorithms in [30], [32]. In this part, we describe a blind equalization techniques for MC-CDMA systems using the algorithms (see Section 1.2) presented above.

2.1. MC-CDMA Transmitter

In the MC-CDMA modulator the complex symbol a_i of each user i is, first, multiplied by each chip $c_{i,k}$ of spreading code, and then applied to the modulator of multicarriers. Each subcarrier transmits an element of information multiply by a code chip of that subcarrier. We consider, for example, the case where the length L_c of spreading code is equal to the number N_p of subcarriers. The optimum space between two adjacent subcarriers is equal to inverse of duration T_c of chip of spreading code in order to guarantee the orthogonality between subcarriers. The MC-CDMA emitted signal is given by

$$x(t) = \frac{a_i}{\sqrt{N_p}} \sum_{q=0}^{N_u-1} \sum_{k=0}^{N_p-1} c_{i,k} e^{2jf_k t}, \tag{29}$$

where $f_k = f_0 + \frac{1}{T_c}$, N_u is the user number and N_p is the number of subcarriers.
We suppose that the channel is time invariant and it's impulse response is characterized by P paths of magnitudes β_p and phases θ_p. So the impulse response is given by

$$h(\tau) = \sum_{p=0}^{P-1} \beta_p e^{j\theta_p} \delta(\tau - \tau_p).$$

The relationship between the emitted signal $s(t)$ and the received signal $r(t)$ is given by: $r(t) = h(t) * x(t) + n(t)$

$$\begin{aligned} r(t) &= \int_{-\infty}^{+\infty} \sum_{p=0}^{P-1} \beta_p e^{j\theta_p} \delta(\tau - \tau_p) x(t-\tau) d\tau + n(t) \\ &= \sum_{p=0}^{P-1} \beta_p e^{j\theta_p} x(t - \tau_p) + n(t), \end{aligned} \tag{30}$$

where $n(t)$ is an additive white Gaussian noise (AWGN).

2.2. MC-CDMA Receiver

The downlink received MC-CDMA signal at the input receiver is given by the following equation

$$\begin{aligned} r(t) = \frac{1}{\sqrt{N_p}} \sum_{p=0}^{P-1} \sum_{k=0}^{N_p-1} \sum_{i=0}^{N_u-1} \times \\ \times \Re \left\{ \beta_p e^{j\theta} a_i c_{i,k} e^{2j\pi (f_0 + k/T_c)(t-\tau_p)} \right\} + n(t), \end{aligned} \tag{31}$$

The equalization goal, is to obtain a good estimation of the symbol a_i. At the reception, we demodulate the signal according the N_p subcarriers, and then we multiply the received sequence by the code of the user. Figure 2 explains the single user-detection principle.

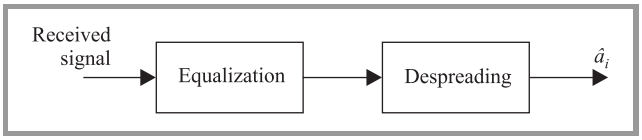


Fig. 2. Principle of the single user-detection.

After the equalization and the spreading operation, the estimation $\hat{a}_i$ of the emitted user symbol a_i, of the i^{th} user can be written by the following equation

$$\begin{aligned} \hat{a}_i &= \sum_{q=0}^{N_u-1} \sum_{k=0}^{N_p-1} c_{i,k} \left(g_k h_k c_{q,k} a_q + g_k n_k \right) \\ &= \underbrace{\sum_{k=0}^{N_p-1} c_{i,k}^2 g_k h_k a_i}_{\text{I}} + \underbrace{\sum_{q=0}^{N_u-1} \sum_{k=0}^{N_p-1} c_{i,k} c_{q,k} g_k h_k a_q}_{\text{II} \quad (q \neq j)} + \underbrace{\sum_{k=0}^{N_p-1} c_{i,k}^2 g_k n_k}_{\text{III}}, \end{aligned} \tag{32}$$

where the term I, II and III of Eq. (32) are, respectively, the desired signal (signal of the considered user), a multiple access interferences (signals of the others users) and the AWGN pondered by the equalization coefficient and by spreading code of the chip. We suppose that the user data are independents and the h_k are ponderated by the g_k equalization coefficient, are independent of the indices k.

3. Equalization for MC-CDMA

3.1. Zero Forcing (ZF)

The principle of the zero forcing technique is to reduce the effect of the fading and the interference while no enhancing effect of the noise on the decision of what data symbol was transmitted. Whenever there is a diversity scheme involved whether it may involve receiving multiple copies of a signal from time, frequency or antenna diversity, the field of classical diversity theory can be applied. These equalization techniques may be desirable for their simplicity as they involve simple multiplications with each copy of the signal. However, they may not be optimal in a channel with interference in the sense of minimizing the error under some criterion. However, the ZF cancels completely the distortions brought by the channel. The gain factor of the ZF equalizer, is given by the equation

$$g_k = \frac{1}{|h_k|}. \tag{33}$$

By that manner, each symbol is multiplied by a unit magnitude. So, the estimated received symbol, $\hat{a}_i$ of symbol a_i of the user i is described by:

$$\hat{a}_i = \underbrace{\sum_{k=0}^{N_p-1} c_{i,k}^2 a_i}_{\text{I}} + \underbrace{\sum_{q=0}^{N_u-1}\sum_{k=0}^{N_p-1} c_{i,k}c_{q,k}a_q}_{\text{II}\quad(q\neq i)} + \underbrace{\sum_{k=0}^{N_p-1} c_{i,k}\frac{1}{h_k}n_k}_{\text{III}}. \quad (34)$$

If we suppose that the spreading code are orthogonal, i.e.,

$$\sum_{k=0}^{N_p-1} c_{i,k}c_{q,k} = 0 \quad \forall i \neq q \quad (35)$$

Eq. (34) will become

$$\hat{a}_i = \sum_{k=0}^{N_p-1} c_{i,k}^2 a_i + \sum_{k=0}^{N_p-1} c_{i,k}\frac{1}{h_k}n_k. \quad (36)$$

Thus, the performance obtained using this detection technique is independent of the users number, if the spreading codes are orthogonal. But, if the h_k value is very weak, (great fading cases), the values g_k increase and the noise will be amplified (second term of Eq. (36)).

3.2. Minimum Mean Square Error, (MMSE)

The MMSE techniques combine the minimization of the multiple access interference and the maximization of signal to noise ratio. Thus as its name indicates, the MMSE techniques minimize the mean square error for each subcarrier k between the transmitted signal x_k and the output detection $g_k r_k$

$$\begin{aligned}\varepsilon[|\varepsilon|^2] &= \varepsilon[|x_k - g_k r_k|^2] \\ &= \varepsilon[(x_k - g_k h_k x_k - g_k n_k)(x_k^* - g_k^* h_k^* x_k^* - g_k^* n_k^*)]. \end{aligned} \quad (37)$$

The minimization of the function $\varepsilon[|\varepsilon|^2]$, gives us the optimal equalizer coefficient, under the minimization of the mean square error criterion, of each subcarrier as

$$g_k = \frac{h_k^*}{|h_k^*|^2 + \dfrac{1}{\gamma_k}}, \quad (38)$$

where $\gamma_k = \dfrac{E[|r_k h_k|^2]}{E|n_k|^2}$.

If the values h_k are small, the SNR for each subcarrier is minimal. So, the use of the MMSE criterion avoid the noise amplification. On the other hand, the greatest values of the h_k and g_k being inversely proportional, allows to restore orthogonality between users. So, the estimated received symbol, $\hat{a}_i$ of symbol a_i of the user i is described by

$$\begin{aligned}\hat{a}_i = &\underbrace{\sum_{k=0}^{N_p-1} c_{i,k}^2 \frac{|h_k|^2}{|h_k|^2 + \frac{1}{\gamma_k}} a_i}_{\text{I}} + \underbrace{\sum_{q=0}^{N_u-1}\sum_{k=0}^{N_p-1} c_{i,k}c_{q,k}\frac{|h_k|^2}{|h_k|^2 + \frac{1}{\gamma_k}} a_q}_{\text{II}\quad(q\neq j)} \\ &+ \underbrace{\sum_{k=0}^{N_p-1} c_{i,k}^2 \frac{h_k^*}{|h_k|^2 + \frac{1}{\gamma_k}} n_k}_{\text{III}}. \end{aligned} \quad (39)$$

The same, if we suppose that the spreading code are orthogonal, i.e.,

$$\sum_{k=0}^{N_p-1} c_{i,k}c_{q,k} = 0 \quad \forall i \neq q \quad (40)$$

Eq. (39) will become

$$\hat{a}_i = \sum_{k=0}^{N_p-1} c_{i,k}^2 \frac{|h_k|^2}{|h_k|^2 + \frac{1}{\gamma_k}} a_i + \sum_{k=0}^{N_p-1} c_{i,k}\frac{h_k^*}{|h_k|^2 + \frac{1}{\gamma_k}} n_k. \quad (41)$$

4. Simulation

4.1. BRAN A Radio Channel

In this subsection we consider the BRAN A model representing the fading radio channels, the data corresponding to this model are measured in an indoor case for multicarrier code division multiple access (MC-CDMA) systems. The following equation describes the impulse response $h_A(n)$ of BRAN A radio channel

$$h_A(n) = \sum_{i=0}^{N_T} h_i \delta(n - \tau_i), \quad (42)$$

where $\delta(n)$ is Dirac function, h_i the magnitude of the targets i, $N_T = 18$ the number of target and τ_i is the time delay (from the origin) of target i. In Table 1 we have summarized the values corresponding the BRAN A radio channel impulse response [27], [28].

Table 1
Delay and magnitudes of 18 targets of BRAN A radio channel

Delay τ_i [ns]	Mag. C_i [dB]	Delay τ_i [ns]	Mag. C_i [dB]
0	0	90	−7.8
10	−0.9	110	−4.7
20	−1.7	140	−7.3
30	−2.6	170	−9.9
40	−3.5	200	−12.5
50	−4.3	240	−13.7
60	−5.2	290	−18
70	−6.1	340	−22.4
80	−6.9	390	−26.7

4.1.1. Blind Channel Impulse Response Estimation of BRAN A

Although, the BRAN A radio channel is constituted by $N_T = 18$ parameters and seeing that the latest parameters are very small. So, in order to estimate the parameters of BRAN A radio channel impulse response, using the max-

imum information obtained by calculating the cumulants function, we take the following procedure:

- We decompose the BRAN A radio channel impulse response into four subchannels as follows:

$$h(n) = \sum_{j=1}^{4} h_j(n); \tag{43}$$

$$h_j(n) = \sum_{i=j}^{P_j} C_j \delta(n-\tau_j); \quad \sum_{j=1}^{4} P_j = N_T\,.$$

- We estimate the parameters of each subchannel, independently, using the proposed algorithms (Alg. 1 and Alg. 2).

- We add all subchannel parameters, to construct the full BRAN A radio channel impulse response.

In Fig. 3 we represent the estimation of the impulse response of BRAN A channel using the proposed algorithms in the case of $SNR = 16$ dB and data length $N = 2048$.

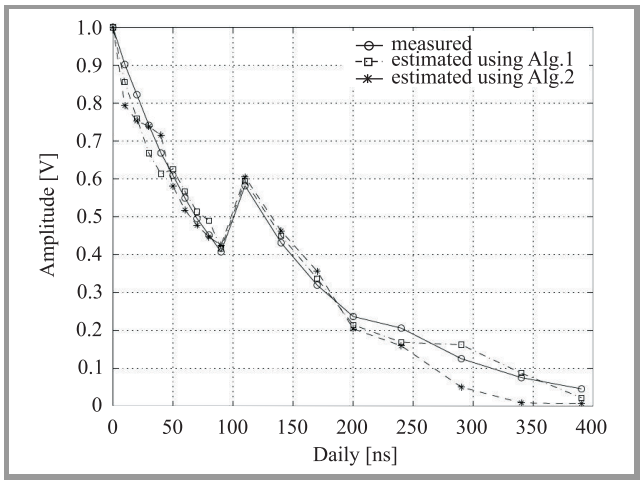


Fig. 3. Estimation of the BRAN A radio channel impulse response for $SNR = 16$ dB and data length $N = 2048$.

From Fig. 3, we can conclude that the algorithm (Alg. 1) gives good estimation for all parameters of BRAN A radio channel impulse response. If we observe the estimated values of BRAN A impulse response, using the algorithm (Alg. 2) shown in Fig. 3, we remark, approximately, the same results given by the Alg. 1 except the last four parameters. Concerning the estimation of BRAN A channel impulse response, for the data length $N = 2048$ and $SNR = 16$ dB, we have a minor difference between the estimated and the measured ones. This result is very interesting for the estimation of impulse response selective frequency channel impulse response in noisy environment. If the data sample increases, we remark that the noise is without influence on the BRAN A radio channel impulse response estimation.

4.2. BRAN E Radio Channel

We have considered in the previous subsection the BRAN A model representing the fading radio channels, where the data corresponding to this model are measured in a scenario of transmission in indoor environment. But in this subsection we consider the BRAN E model representing the fading radio channels, where the model parameters are measured in outdoor scenario. The Eq. (44) describes the impulse response of BRAN E radio channel.

$$h_E(n) = \sum_{i=0}^{N_T} h_i \delta(n-\tau_i)\,, \tag{44}$$

where $\delta(n)$ is Dirac function, h_i the magnitude of the target i, $N_T = 18$ the number of targets and τ_i is the delay of target i. In Table 2 we have represented the values corresponding to the BRAN E radio channel impulse response.

Table 2
Delay and magnitudes of 18 targets of BRAN A channel

Delay τ_i [ns]	Mag. C_i [dB]	Delay τ_i [ns]	Mag. C_i [dB]
0	−4.9	320	0
10	−5.1	430	−1.9
20	−5.2	560	−2.8
40	−0.8	710	−5.4
70	−1.3	880	−7.3
100	−1.9	1070	−10.6
140	−0.3	1280	−13.4
190	−1.2	1510	−17.4
240	−2.1	1760	−20.9

4.2.1. Blind Channel Impulse Response Estimated of BRAN E

Seeing that the BRAN E radio channel is composed by $N_T = 18$ parameters and seeing that the latest parameters are very small. So, in order to estimate the parameters of the BRAN E radio channel impulse response with maximum information obtained by calculating the cumulants function, we take the same procedure used in BRAN A radio channel such as decomposing the BRAN E impulse response into four subchannels, and then we estimate each subchannel parameters using the proposed algorithms. This procedure gives a good estimation of the impulse response channel. The same, in time domain, we represent the BRAN E radio channel impulse response parameters (Fig. 4) for data length $N = 2048$ and for $SNR = 16$ dB.
From Fig. 4, we can conclude that the estimated BRAN E channel impulse response, using the algorithm Alg. 1, is very closed to the true one, for data length $N = 2048$ and $SNR = 16$ dB. But, the values given by the second algorithm (Alg. 2) have the same form comparing to those

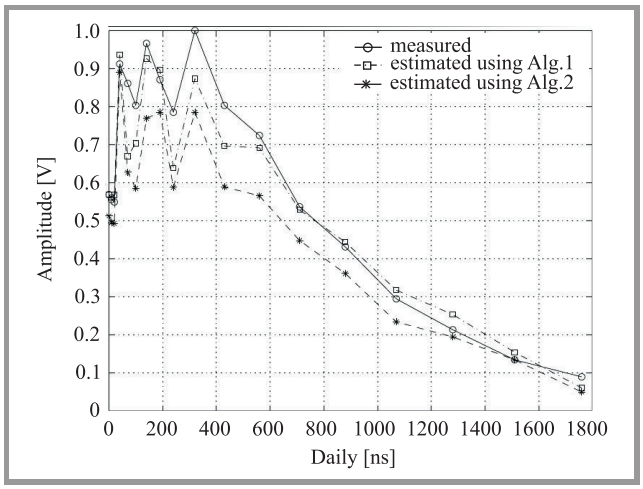


Fig. 4. Estimation of the BRAN E radio channel impulse response for an $SNR = 16$ dB and a data length $N = 2048$.

measured, with a light difference. This is because the BRAN E impulse response have more fluctuations comparing to BRAN A. This result is very interesting for the estimation of selective frequency channel impulse response in noisy environment.

5. MC-CDMA System Performance

In order to evaluate the performance of the MC-CDMA systems, using the proposed algorithms, we consider the BER, for the two equalizers ZF and MMSE, using measured and estimated (using the proposed algorithms) BRAN A and BRAN E channel impulse responses. The results are evaluated for different values of SNR.

5.1. ZF and MMSE Equalizers: Case of BRAN A Channel

In Fig. 5, we represent the BER for different SNR, using the measured and estimated BRAN A channel but the equalization is performed using the ZF equalizer. Figure 6 represents the BER for different SNR, using the measured and estimated BRAN A channel but the equalization is performed using the MMSE equalizer.

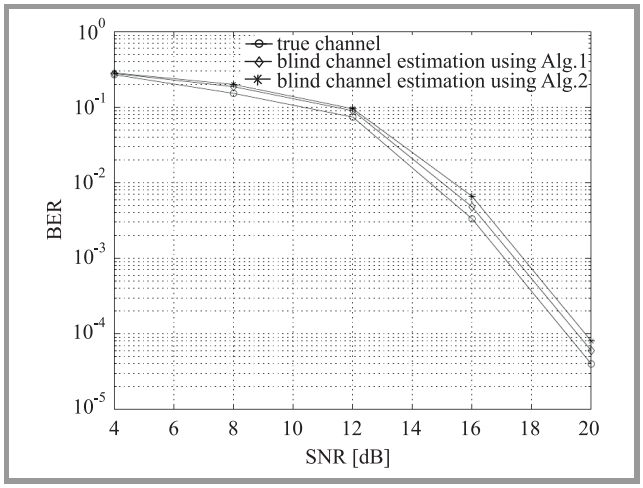


Fig. 5. BER of the estimated and measured BRAN A channel using the ZF equalizer.

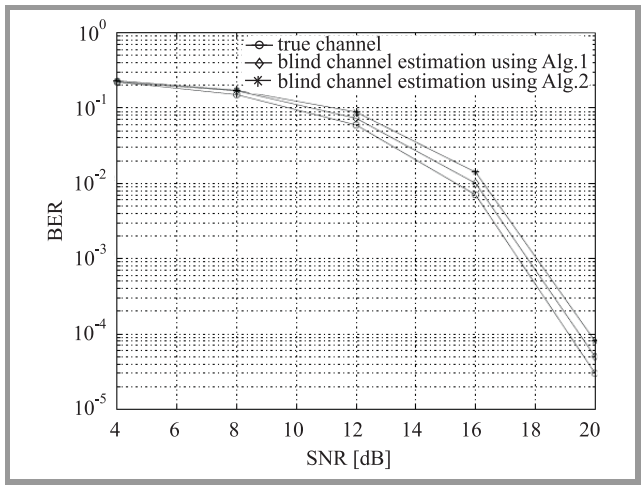


Fig. 6. BER of the estimated and measured BRAN A channel using the MMSE equalizer.

The BER simulation for different SNR, demonstrates that the estimated values by the first algorithm (Alg. 1) are more close to the measured value than those estimated by second algorithm (alg. 2). From Fig. 5, we conclude that: if the $SNR = 20$ dB we have a BER less than 10^{-4}, but using the MMSE equalizer we have only the BER less than 10^{-5}. This is because MMSE equalizer best than the ZF technique. In real case, and in abrupt channel, the proposed blind identification techniques can be useful as remarked in Figs. 5 and 6.

5.2. ZF and MMSE Equalizers: Case of BRAN E Channel

We represent in Fig. 7, the simulation results of BER estimation using the measured and blind estimated of the

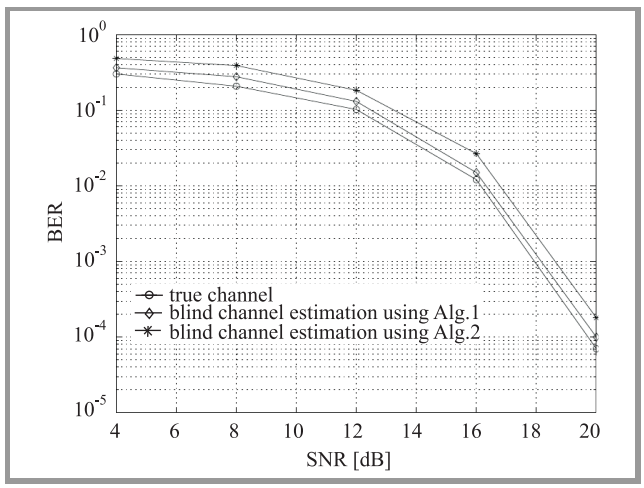


Fig. 7. BER of the estimated and measured BRAN E channel using ZF equalizer.

BRAN E channel impulse response. The equalization is performed using ZF equalizer. Figure 7 demonstrates clearly that the BER obtained using the estimated values by algorithms (Alg. 1 and alg. 2) for ZF equalization is like this obtained using measured values for ZF equalization. Both the two techniques give the 1 bit error if we receive 10^4 bits for a $SNR = 20$ dB.

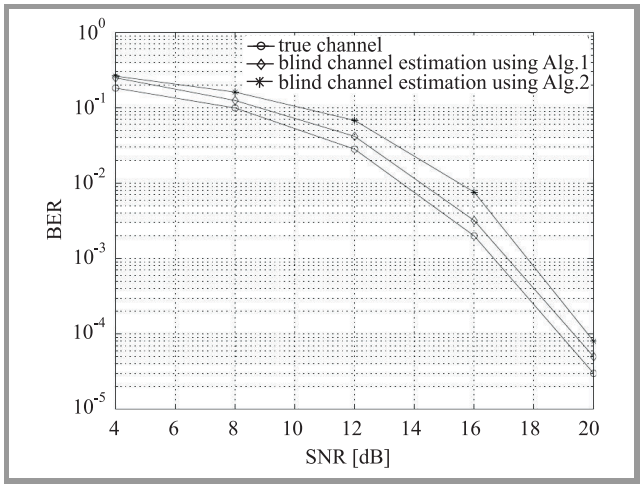


Fig. 8. BER of the estimated and measured BRAN E channel using MMSE equalizer.

In the same manner, we represent in Fig. 8 the simulation results of BER estimation using the measured and blind estimated of the BRAN E channel impulse response. The equalization is performed using MMSE equalizer. From Fig. 8, we observe that the blind MMSE equalization gives approximately the same results obtained using the measured BRAN E values for MMSE equalization. So, if the *SNR* values are superior to 20 dB, we observe that 1 bit error occurred when we receive 10^5 bits, but if the $SNR \geq 20$ dB we will obtain only one bit error occurred for 10^6 bits received.

6. Conclusion

In this paper we have presented two algorithms based on third and fourth order cumulants to identify the parameters of the impulse response of the frequency selective channel such as the experimental channels, BRAN A and BRAN E. The simulation results show the efficiency of these algorithms, mainly if the input data are sufficient. The magnitude of the impulse response is estimated with an acceptable precision in noisy environment, mainly, in the case of small number of samples. For the equalization of the MC-CDMA systems, we have obtained good results on bit error rate principally if we use the first algorithm (Alg. 1) based on third cumulants.

References

[1] S. Safi and A. Zeroual, "Modelling solar data using high order statistics", *J. Stat. Comp. Simul., A.M.S.E., Adv. Modell. Anal.*, vol. 6, no. 2, pp. 1–16, 2002.

[2] S. Safi and A. Zeroual, "MA system identification using higher order cumulants: application to modelling solar radiatio", *J. Stat. Comp. Simul., Taylor & Francis*, vol. 72, no. 7, pp. 533–548, 2002.

[3] S. Safi and A. Zeroual, "Blind identification in noisy environment of non-minimum phase Finite Impulse Response (FIR) using higher order statistics", *Int. J. Sys. Anal. Modell. Simul., Taylor & Francis*, vol. 43, no. 5, pp. 671–681, 2003.

[4] S. Safi and A. Zeroual, "Blind parametric identification of linear stochastic non-Gaussian FIR systems using higher order cumulants", *Int. J. Sys. Sci., Taylor & Francis*, vol. 35, no. 15, pp. 855–867, 2004.

[5] S. Safi, J. Antari, A. Zeroual, and A. Lyhyaoui, "Parametric identification of linear finite impulse response non-Gaussian systems using higher order cumulants", in *Proc. Inf. Commun. Technol. Int. Symp. ICTIS'2005*, Tetuan, Morocco, 2005, pp. 317–322.

[6] S. Safi and A. Zeroual, "Blind non-minimum phase channel identification using 3rd and 4th order cumulants", *Int. J. Sig. Proces.*, vol. 4, no. 2, pp. 158–167, 2007.

[7] B. Sadler, G. B. Giannakis, and K.-S. Lii, "Estimation and detection in the presence of non-Gaussian noise", *IEEE Trans. Sig. Proces.*, vol. 42, no. 10, pp. 2729–2741, 1994.

[8] W. Robert, Jr. Heath, and G. B. Giannakis, "Exploiting input cyclostationarity for blind channel identification in OFDM systems", *IEEE Trans. Sig. Proces.*, vol. 47, no. 3, pp. 848–856, 1999.

[9] M. Boumahdi, F. Glangeaud, and J. L. Lacoume, "Déconvolution aveugle en sismique utilisant les statistiques d'ordre supérieur", in Proc. 14th GRETSI Symposium, Juan-Les-Pins, France, 1993, pp. 89–92.

[10] K. D. Kammeyer and B. Jelonnek, "A new fast algorithm for blind MA-system identification based on higher order cumulants", in *SPIE Adv. Sig. Proc. Algorithms, Architectures and Implementations*, San Diego, Spain, 1994.

[11] D. Boss, B. Jelonnek, and K. D. Kammeyer, "Decision-feed back eigenvector approach to blind ARMA equalization and identification", in *Proc. IEEE-SP/ATHOS Worksh. Higher Order Stat.*, Girona, Spain, 1995.

[12] S. A. Ashbeili, M. T. Ozgen, A. E. Cetin, and A. N. Venetsapoulos, "Cumulant-based parametric multichannel FIR system identification methods", in *Proc. IEEE Sig. Proces. Worksh. Higher Order Stat.*, South Lake Tahoe, USA, 1993, pp. 200–204.

[13] J. K. Tugnait, "Approaches to FIR system identification with noisy data using higher order statistics", *IEEE Trans. ASSP*, vol. 38, no. 1, pp. 1307–1317, 1990.

[14] A. Swami, and J. Mendel, "Closed form recursive estimation of MA coefficients using autocorrelation and third order cumulants", *IEEE ASSP*, vol. 37, no. 11, 1989.

[15] S. Safi and A. Zeroual, "Modelling solar data using high order statistic techniques: new method proposed", in *Proc. Int. Conf. Model. Simul. MS'99*, Santiago de Compostela, Spain, 1999, vol. II, pp. 157–167.

[16] R. Pan and C. L. Nikias, "The complex cepstrum of higher order cumulants and non minimum phase system identification", *IEEE Trans. ASSP*, vol. 36, no. 2, 1988.

[17] B. Friedlander and B. Porat, "Asymptotically optimal estimation of MA and ARMA parameters of non-Gaussian processes from high-order moments", *IEEE Trans. Autom. Control*, vol. 35, no. 1, pp. 27–37, 1990.

[18] C. L. Nikias, "ARMA bispectrum approach to non minimum phase system identification", *IEEE Trans. ASSP*, vol. 36, no. 4, 1988.

[19] J. K. Tugnait, "Identification of non-minimum phase linear stochastic systems", *Automatica*, vol. 22, no. 4, pp. 487–464, 1986.

[20] J. K. Tugnait, "Identification of linear stochastic systems via second and fourth order cumulant matching", *IEEE Trans. Info. Theory*, vol. 33, no. 3, 393–407, 1987.

[21] S. Safi, A. Zeroual, and M. M. Hassani, "Parametric identification of non-Gaussian signals using diagonal slice cumulants, application to modelling solar process", in *Proc. Microwave Symp. MS'2000*, Tetouan, Morocco, 2000, pp. 345–350.

[22] W. Jun and H. Zhenya, "Criteria and algorithms for blind source separation based on cumulan", *Int. J. Electron.*, vol. 81, no. 1, pp. 1–14, 1996.

[23] L. Ju and H. Zhenya, "Blind identification and equalization using higher-order cumulants and ICA algorithms", in *Proc. Int. Conf. "Neural Networks and Brain ICNNB'98*, Beijing, China, 1998.

[24] G. B. Giannakis and J. Mendel, "Cumulant-based order determination of non-Gaussian process ARMA models", *IEEE Trans. ASSP*, vol. 38, pp. 1411–1422, 1993.

[25] J. R. Fonollosa and C. L. Nikias, "Wigner higher-order moment spectra: definitions, properties, computation and applications to transient signal detection", *IEEE Trans. Sig. Proces.*, vol. 41, no. 1, pp. 245–266, 1993.

[26] X. D. Zhang and Y. S. Zhang, "FIR system identification using higher order statistics alone", *IEEE Trans. Sig. Proces.*, vol. 42, no. 12, pp. 2854–2858, 1994.

[27] ETSI TS 101 475 V1.3.1, "Broadband Radio Access Networks (BRAN), HIPERLAN Type 2, Physical (PHY) layer", 2001.

[28] ETSI TR 101 031 V2.2.1, "Broadband Radio Access Networks (BRAN), (HIPERLAN) Type 2", Requirements and architectures for wireless broadband access, 1999.

[29] J. M. Kahn and K.-P. Ho, "Spectral efficiency limits and modulation/detection techniques for DWDM systems", *IEEE. J. Sel. Topics in Quant. Electron*, vol. 10, pp. 259–272, 2004.

[30] J.-P. M. G. Linnartz, "Performance analysis of synchronous MC-CDMA in mobile rayleigh channel with both delay and doppler spreads", *IEEE Trans. Veh. Technol.*, vol. 50, no. 6, 2001.

[31] J. M.-M. Anderson and G. B. Giannakis, "Noisy input output system identification using cumulants and the Streiglitz-McBride algorithm", *IEEE Trans. Sig. Proces. Mag.*, vol. 44, no. 4, pp. 1021–1024, 1996.

[32] S. Kaiser, "OFDM-CDMA versus DS-CDMA: performance evaluation for fading channels", in *Proc. IEEE Int. Conf. Communications ICC'95*, Seattle, USA, 1995, pp. 1722–1726.

[33] J. G. Proakis, *Digital Communications*. New York: Mc Graw Hill, 2000.

[34] I. Cosovic, M. Schnell, and A. Springer, "Combined pre- and post-equalization for uplink time division duplex MC-CDMA in fading channels", in P*roc. Int. Worksh. Multi-Carrier Spread-Spectrum MC-SS'03*, Wessling, Germany, 2003, pp. 439–450.

[35] R. Le Couable and M. Helard, "Perforamnce of single and multi-user detection techniques for MC-CDMA system over channel model used for HIPERLAN2", in *Proc. IEEE Spread-Spectrum Techniq. Appl.*, Parsippany, New Jersey, 2000, pp. 718–722.

[36] S. Verdu, *Multiuser Detection*. Cambrigde: Cambridge University Press, 1998.

[37] N. Yee, J.-P. M. G. Linnartz, and G. Fettweis, "Multi-carrier-CDMA in indoor wireless networks", in *Proc. Conf. PIMRC'93*, Yokohama, Japan, 1993, pp. 109–113.

[38] C. L. Nikias and J. M. Mendel, "Signal processing with higher order spectra", *IEEE Sig. Proces. Mag.*, vol. 10, pp. 10–37, 1993.

[39] L. Srinivas and K. V. S. Hari, "FIR system identification using higher order cumulants: a generalized approach", *IEEE Trans. Sig. Proces.*, vol. 43, no. 12, pp. 3061–3065, 1995.

[40] Y. Xiao, M. Shadeyda, and Y. Tadokoro, "Over-determined $C(k,q)$ formula using third and fourth order cumulants", *Eletron. Lett.*, vol. 32, pp. 601–603, 1996.

[41] X. D. Zhang and Y. S. Zhang, " Singular value decomposition-based MA order determination of non-Gaussian ARMA models", *IEEE Trans. Sig. Proces.*, vol. 41, pp. 2657–2664, 1993.

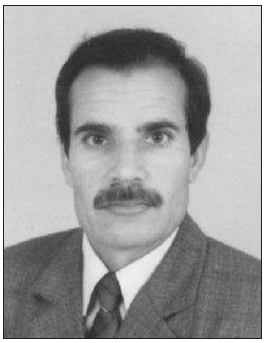
[42] S. Safi, "Identification aveugle des canaux à phase non minimale en utilisant les statistiques d'ordre supérieur: application aux réseaux mobiles". Thèse d'Habilité, Cadi Ayyad University, Marrakesh, Morocco, 2008.

Said Safi was born in Beni Mellal, Morocco in 1971, received the B.Sc. degree in physics (option electronics) from Cadi Ayyad University, Marrakech, Morocco in 1995, M.Sc. and Doctorate degrees from Chouaib Doukkali University and Cadi Ayyad University, Morocco, in 1997 and 2002, respectively. He has been a professor of information theory and telecommunication systems at the National School for Applied Sciences, Tangier Morocco, from 2003 to 2005. Since 2006, he is a professor of applied mathematics and programming at the Faculty of Science and Technics, Beni Mellal Morocco. In 2008 He received the Ph.D. degree in telecommunication and informatics from the Cadi Ayyad University. His general interests span the areas of communications and signal processing, estimation, time-series analysis, and system identification – subjects on which he has published 10 journal papers and more than 40 conference papers. Current research topics focus on transmitter and receiver diversity techniques for single- and multi-user fading communication channels, and wide-band wireless communication systems.
e-mail: safi.said@gmail.com
Polydisciplinary Faculty
Sultan Moulay Slimane University
Po. Box. 523
Beni Mellal, Morocco

Miloud Frikel received his Ph.D. degree from the center of mathematics and scientific computation CNRS URA 2053, France, in array processing. Currently, he is with the GREYC laboratory and the ENSICAEN as assistant professor. From 1998 to 2003 he was with the Signal Processing Lab, Institute for Systems and Robotics, Institute Superior Tecnico, Lisbon, as a researcher in the field of wireless location and statistical array processing, after been a research engineer in a software company in Munich, Germany, and he worked in the Institute for Circuit and Signal Processing of the Technical University of Munich, Germany. Dr. Frikel's research interests span several areas, including statistical signal and array processing, cellular geolocation (wireless location), space-time coding, direction finding and source localization, blind channel identification for wireless communication systems, and MC-CDMA systems.
e-mail: mfrikel@greyc.ensicaen.fr
GREYC UMR 6072 CNRS
ENSICAEN
6, B. Maréchal Juin
14050 Caen, France

Mohammed M'Saad was educated at Mohammadia School of Engineering in Rabat, Morocco, where he held an Assistant Professor position in 1978. He held a research position at the Laboratoire d'Electronique et d'Etude des Systémes in Rabat, where he prepared his doctor engineering degree in process control. In November 1982, he joined the Laboratoire d'Automatique de Grenoble to work on theory and applications of adaptive control. He received his Doctorat d'Etates- Sciences Physiques from the Institut National Polytechnique de Grenoble in April 1987. In March 1988, he held a research position at the Centre National de Recherche Scientifique. In September 1996, he held a Professor position at the Ecole Nationale Supérieure d'Ingénieurs de Caen, where he is the Head of the Control Group at the GREYC. His main research areas are adaptive control theory, system identification and observation, advanced control methodologies and applications, computer aided control engineering.

e-mail: mohammed.msaad@greyc.ensicaen.fr
GREYC UMR 6072 CNRS
ENSICAEN
6, B. Maréchal Juin
14050 Caen, France



Abdelouhab Zeroual is Professor in the Department of Physics at the Faculty of Sciences Semlalia, Cadi Ayyad University, Marrakesh, Morocco. He received the D.E.S. and the Ph.D. in signal processing from the Cadi Ayyad University, Morocco, respectively in 1988 and 1995. Review in many international journals and he is currently a supervisor of several research works. He has published more than 30 papers in international journal and more than 100 papers in international conferences. His research interests include statistical signal processing, modeling, linear and nonlinear system identication, blind equalization and solar energy systems.

e-mail: zeroual@ucam.ac.ma
Department of Physics
Faculty of Sciences Semlalia
Cadi Ayyad University
Marrakesh, Morocco

Paper

Characteristics of Measured Rainfall Rate at Ogbomoso, Nigeria for Microwave Applications

F. A. Semire[a] and T. I. Raji

[a] Department of Electronic and Electrical Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria

Abstract—Characteristics of rainfall rate useful in the estimation of attenuation due to rain are presented. Rain data collected at Ogbomoso between January–October, 2009 were used in the analysis. Result shows that power law relationship exists between the equiprobable rain rates of two different integration times. The value of conversion factor C_E and C_R obtained for Ogbomoso are 0.28(60) and 0.64(90) respectively. Our result then shows that different conversion factor is required for different location even within the same climatic region.

Keywords—characteristics, Ogbomoso, rainfall.

1. Introduction

With the rapid development currently being witnessed in the field of information technology there is an increasing demand for broadband satellite services and this has called for satellite system that can provide rapid and reliable transmission of information from one end to another. Attenuation due to rain is one of the factors that limits the path length over which reliable radio communication systems can be established. It also limits the usage of higher frequencies for terrestrial microwave point to point as well as satellite communication. As the frequency increases, so does the impact of atmospheric conditions on the radio wave propagation [1], which causes reduction in the quality of signal in the case of analog transmissions, and increase in the bit error rate in the case of digital transmission.

In this paper, some characteristic of tropical rainfall as measured at Ogbomoso are discussed using rainwise rain-guage between January–October 2009. The effect of integration time on the rain rate and cumulative distribution functions are examined. Rain rate duration characteristics are also discussed.

2. Measurement System

The precise knowledge of rain attenuation on any communication link improves the estimation of link availability which provides accurate knowledge of outage time excepted. Most attenuation prediction models required at least 1 min rain rate statistic [2]–[4]. Rain rate statistics is specified on a percentage of time basis, that is the percentage of time in a year or a month that the rain rate equals or exceeds a specific value.

The experimental set-up for this measurement of rain rate characteristic is located at Ladoke Akintola University of Technology, Ogbomoso. The rain rate are measured using rainwise tipping bucket rain guage of 0.5 mm per tip at different integration time. The cumulative distributions of rain rate for different integration times are generated from rain data base.

3. Results of Rain Rate Measurement in Ogbomoso

3.1. Integration Time

The relationship between rain rate statistics with different integration times has been studied from the results obtained from the rain gauge. The cumulative distribution of the rain rate from the different integration times generated from the rain gauge data is shown in Table 1 and the corresponding graph in Fig. 1.

Table 1
Time rain rate exceeded for different integration times

Rain rate [mm/hr]	Percentage of rain rate is exceeded for integration time			
	1 min	5 min	10 min	20 min
210	0.0064	0.0206	0.0386	0.110
180	0.00704	0.0123	0.0193	0.0787
150	0.0094	0.0185	0.0579	0.0866
120	0.0200	0.0699	0.143	0.236
90	0.0276	0.0864	0.135	0.307
60	0.0745	0.302	0.394	0.551
30	0.871	2.366	2.812	4.567

At the low availabilities, the probability of raining is an important parameter determining the annual outage time percentage, below which the rain attenuation has to be considered in the link to be designed [5]. From the cumulative distribution above, a table from which the relationship between equiprobable rain rates for the different integration times is established. This involves developing a conversion method for time probability of one minute rainfall rate from that for integration time great than one-minute. The result is shown in Table 2 and Fig. 2.

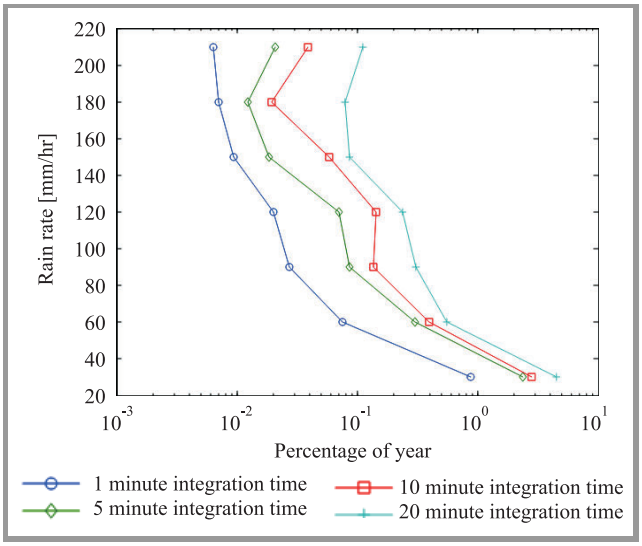


Fig. 1. Cumulative distributions of rain rate at Ogbomoso for different integration times between January and October 2009.

Table 2
Value for equiprobable rain rates for different integration times

$R_{1\min}$ [mm/hr]	R_τ [mm/hr]		
	5 min	10 min	20 min
30	22	16	10
60	42	29	22
90	61	47	35
120	79	62	49
150	97	78	64
180	114	93	79
210	131	108	95

3.2. Conversion Factors

According to G.O. Ajayi *et al.* and Watson *et al.* [6]–[7], conversion factors C_R and C_e for different integration times are considered as:

$$C_R(t) = \frac{R_T}{R_\tau},$$

$$C_e(R) = \frac{e_T}{e_\tau},$$

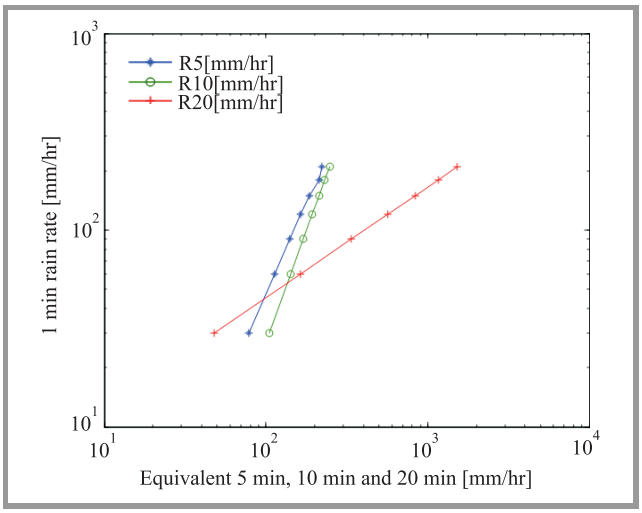


Fig. 2. Equivalent 1-min rain rate for different integration times at equal probabilities of occurrence.

where C_R is the ratio of rain rates exceeded for a given percentage of time t as measured by the rain gage with integration times T and τ, C_e is the ratio of the exceedances for a given rain rate measured using the integration time T.

The result of C_e obtained in Ogbomoso for $T = 5$ min and $\tau = 1$ min was then compared with that obtained in Ile-Ife and some countries in Europe. The result is shown in Table 3.

As shown in Table 3 there is a gradual decrease in the value of C_e with increasing rain rate for the European countries while that of Ile-Ife and Ogbomoso in Nigeria decreases rapidly with increasing rain rate. This suggests that C_e might be climate dependent as suggested in [8] which is also corroborated as according to the value obtained for Ogbomoso. The value of C_R obtained in Ogbomoso is also compared with that obtained in [7] for some stations in Europe and that of Ile-Ife, as obtained in [6]. The results obtained in Ogbomoso agrees with that obtained in Ile-Ife which are generally lower than values obtained for other European stations. On the average, the percentage difference between the values of C_R obtained for Europe and other temperate regions are generally lower than that obtained in tropical regions such as Ogbomoso and Ile-Ife. The values are depicted in Table 4.

3.3. Return Periods

Return periods for specific rain data were studied from the rain data we obtained here in Ogbomoso over the period between January and October 2009. Table 5 shows the number of occasions when rain rates of 30, 60, 90, 120, 150, 180 and 210 mm/hr had particular return periods. It is shown also in Fig. 3.

Table 3
Values of $C_e(R)$ for $T = 5$ min and $\tau = 1$ min

Location	Rainfall rate [mm/hr]									Comments
	10	20	30	40	50	60	70	80	90	
Greece							0.65	0.51		2 year data for Keffalina
Italy			0.63	0.60	0.60		0.63			2 year data from Rome
West Germany		0.80	0.74	0.73						1 year data from Darmstadt
UK	0.78	0.72	0.71	0.69	0.60		0.43			5 year data from southern UK on a network of rain gauges
Nigeria (Ile-Ife)	0.74	0.68	0.59	0.57	0.40	0.30	0.17	0.10	0.08	28-month data obtained at Ile-Ife using a fast response rain gauge
Nigeria (Ogbomoso)			0.37			0.28			0.16	10-month data obtained at Ogbomoso using a rain gauge
All results except Nigeria (Ogbomoso) was obtained from [6].										

Table 4
Values of $C_R(R)$ for $\tau = 1$ min numbers in bracket indicate the 1 min rain rate

Location	T [min]	Percentage of year		Comments
		0.01	0.001	
Italy	5	0.8(100)		2 year data from Rome
	10	0.7(100)		
	60	0.42(100)		
UK	5	0.84(20)	0.82(60)	5 year data from southern UK from a network of rain gauges
	10	0.77(20)	0.72(60)	
	60	0.59(20)		
West Germany	5	0.93(20)	0.9(40)	1 year data from Darmstadt
	10	0.81(20)		
Nigeria (Ile-Ife)	5	0.68(80)	0.64(130)	28-month data obtained at Ile-Ife
	10	0.52(80)	0.53(130)	
Nigeria (Ogbomoso)	5	0.64(90)		10-month data obtained at Ogbomoso
	10	0.53(90)		

Table 5
Values of return periods at different rain rate

Rain rate [mm/hr]	Return period	No. of occasions rain rate was exceeded
30	0.010	1484
	0.423	1150
	0.356	728
	0.222	573
60	3.311	147
	1.147	127
	2.538	102
	1.815	70
90	37.017	46
	11.574	42
	1.815	39
	7.407	35
120	6.993	37
	50.075	34
	4.237	30
150	106.383	16
	17.271	15
	11	11
180	9	9
	142.045	12
	7.134	10
	81.301	6
	51.815	5
210	9.091	14
	156.25	11
	48.543	10

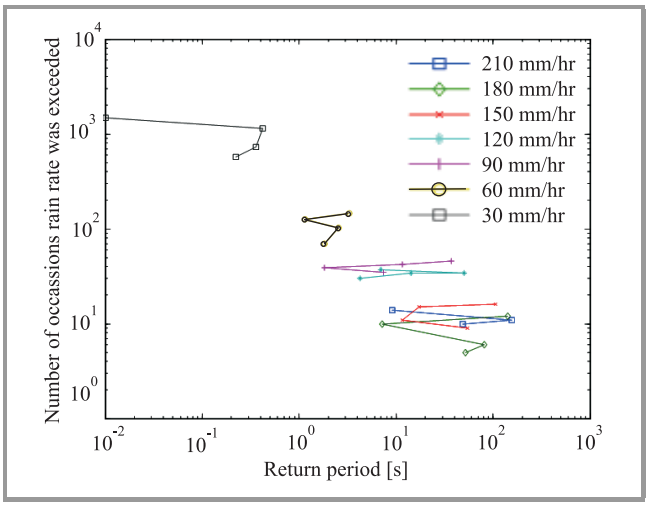


Fig. 3. Characteristics of return period of rain rates.

3.4. Rain Duration

The rain rate duration data are paramount to study the characteristics of precipitation. The data is useful in the determination of communication link outage due to rainfall. The rain duration at different rain rates is shown in Table 6 and the corresponding graphs in Figs. 4 and 5.

Table 6
Rain duration at different rain rates

Rain rate [mm/hr]	No. of occasions rain rate was exceeded	Rain duration [s]
30	6	360
Different rain events at which rain volume is greater than or equal to 100 mm	8	480
	11	660
	20	1200
	29	1740
	31	1860
	46	2760
	52	3120
	134	8040
60	1	60
	3	180
	4	240
	7	420
	8	480
	9	540
	11	660
	14	840
90	1	60
	2	120
	3	180
	5	300
	7	420
	8	540
120	1	60
	2	120
	3	180
	4	240
	9	540
150	1	60
	2	120
	4	240
	6	360

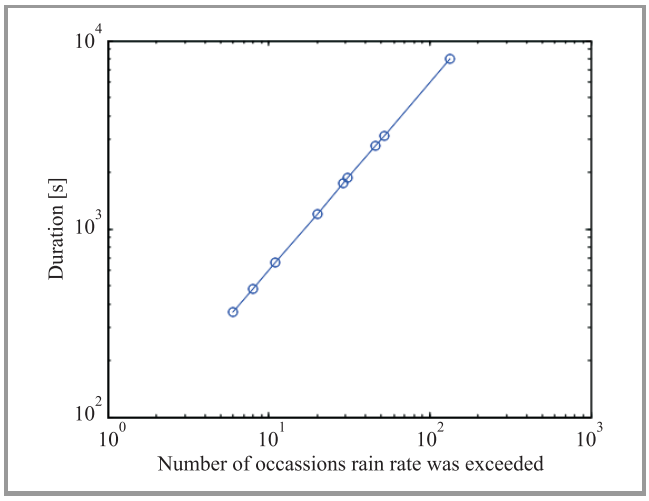


Fig. 4. Rain duration at 30 mm/hr rain rate.

4. Conclusion

In this contribution, rainfall rate data between January-October, 2009 at Ogbomoso have been used in the study of effect of integration time on the cumulative distribution of rain rate. The result shows that power law relationship exists between the equiprobable rain rates of two different integration times. Our result compared to Ile-Ife follows the same trend except that the value obtained in Ogbomoso is a little higher than Ile-Ife. Although, Ile-Ife rain rate is expected to be higher because Ogbomoso experiences Northern climatic condition. Therefore it is recommended that the work of [6] need to be revisited as a result of change in climatic condition due effect of global warming. The conversion factors C_R and C_E obtained at Ogbomoso are lower as compared to those obtained at Ile-Ife. The value of C_E and C_R obtained for Ogbomoso are 0.28(60) and 0.64(90) respectively. Our results show that different conversion factor is required for different locations even within the same climatic region for the conversion of one integration time to another. However, measurement period of 10 months may not be sufficiently enough to compare other literature results. Further detailed analysis based on longer period would be performed and presented by the authors in the future.

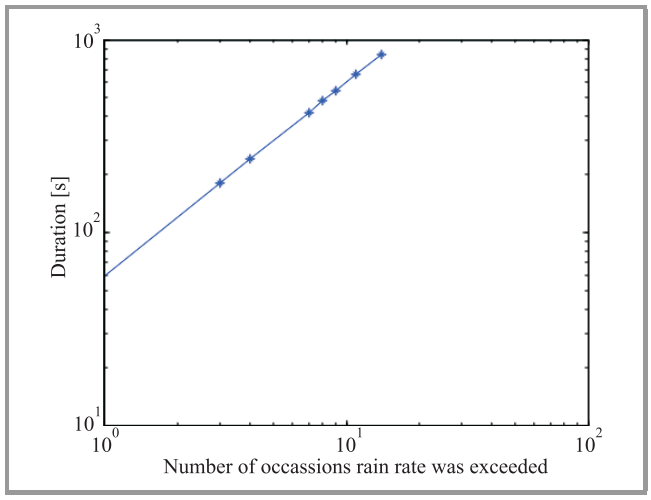


Fig. 5. Rain duration at 60 mm/hr rain rate.

References

[1] L. J. Ippolito Jr., *Radiowave Propagation in Satellite Communication*. New York: Van Nostrand Reinhold Company, 1986.

[2] "Propagation data and prediction methods requirement for the design of Earth-space", ITU-RP. 618-10.

[3] S. H. Lin, "National long term rain statistics and empirical calculate of 11 GHz microwave rain attenuation", *The Bell Syst. Techn. J.*, vol. 56, no. 9, pp. 1581–1604, 1997.

[4] S. H. Lin, "A method for calculating rain attenuation distributions on microwave paths", T*The Bell Syst. Techn. J.*, vol. 54, pp. 1051–1086, 1975.

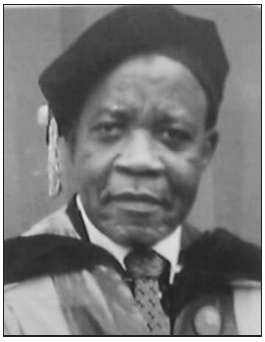
[5] "Specific attenuation models for rain for use in prediction methods", ITU-R Rec. P. 838-3.

[6] G. O. Ajayi and E. B. Ofoche "Some tropical rainfall rate characteristic at Ile-Ife for microwave and millimetre wave applications", *J. Climate Appl. Meteorol.*, no. 23, pp. 562–567, 1983.

[7] P. A. Watson, V. Sathiaseelan, and B. Potter, "Development of a climatic map of rainfall attenuation for Europe", Post Graduate School of Electrical and Electronic Engineering, University of Braford, U.K., Rep. no. 300, p. 134, 1981.

[8] G. O. Ajayi,"Statistical properties of tropical rainfall intensity measured at Ile-Ife, a southern station in Nigeria for microwave and millimetre wave applications", *Ann. Teelecommun.*, no. 37, pp. 477–483, 1982.

F. A. Semire had her B.Sc. in electrical and electronic engineering at Ladoke Akintola University of Technology (LAUTECH), Ogbomoso, Nigeria in 2000. She completed her M.Sc. in communication option from University of Lagos, Nigeria in 2003. She is currently working in the Department of Electronic and Electrical Engineering, LAUTECH and pursuing her Ph.D. in the field of radio propagation (rain attenuation) at University Science Malaysia.
e-mail: semireban@yahoo.com
Department of Electronic and Electrical Engineering
Ladoke Akintola University of Technology
Ogbomoso, Nigeria



T. I. Raji had his B.Sc. and M.Sc. in electrical engineering at Columbia University, New York, USA, between 1962 and 1967. He proceeded to University of Roschester, New York, for his Ph.D. in electrical engineering from 1970 to 1975. He started his teaching career as a teaching assistant in the Department of Electrical Engineering, University of Rochester from 1970 to 1972. He joined Obefemi Awolowo University (OAU), Ile-Ife, Nigeria, in 1975 as a lecturer and rose to the position of senior lecturer 1979. He later transferred his service to Ladoke Akintola University of Technology, Ogbomoso, where he became a Professor in 1990. He died on 2nd of November, 2010.

Information for Authors

Journal of Telecommunications and Information Technology **(JTIT)** is published quarterly. It comprises original contributions, dealing with a wide range of topics related to telecommunications and information technology. **All papers are subject to peer review**. Topics presented in the JTIT report primary and/or experimental research results, which advance the base of scientific and technological knowledge about telecommunications and information technology.

JTIT is dedicated to publishing research results which advance the level of current research or add to the understanding of problems related to modulation and signal design, wireless communications, optical communications and photonic systems, voice communications devices, image and signal processing, transmission systems, network architecture, coding and communication theory, as well as information technology.

Suitable research-related papers should hold the potential to advance the technological base of telecommunications and information technology. Tutorial and review papers are published only by invitation.

Manuscript. TEX and LATEX are preferable, standard Microsoft Word format (.doc) is acceptable. The author's JTIT LATEX style file is available:
http://www.nit.eu/for-authors

Papers published should contain up to 10 printed pages in LATEX author's style (Word processor one printed page corresponds approximately to 6000 characters).

The manuscript should include an abstract about 150–200 words long and the relevant keywords. The abstract should contain statement of the problem, assumptions and methodology, results and conclusion or discussion on the importance of the results. Abstracts must not include mathematical expressions or bibliographic references.

Keywords should not repeat the title of the manuscript. About four keywords or phrases in alphabetical order should be used, separated by commas.

The original files accompanied with pdf file should be submitted by e-mail: redakcja@itl.waw.pl

Figures, tables and photographs. Original figures should be submitted. Drawings in Corel Draw and PostScript formats are preferred. Figure captions should be placed below the figures and can not be included as a part of the figure. Each figure should be submitted as a separated graphic file, in .cdr, .eps, .ps, .png or .tif format. Tables and figures should be numbered consecutively with Arabic numerals.

Each photograph with minimum 300 dpi resolution should be delivered in electronic formats (TIFF, JPG or PNG) as a separated file.

References. All references should be marked in the text by Arabic numerals in square brackets and listed at the end of the paper in order of their appearance in the text, including exclusively publications cited inside. Samples of correct formats for various types of references are presented below:

[1] Y. Namihira, "Relationship between nonlinear effective area and mode field diameter for dispersion shifted fibres", *Electron. Lett*., vol. 30, no. 3, pp. 262–264, 1994.

[2] C. Kittel, *Introduction to Solid State Physics*. New York: Wiley, 1986.

[3] S. Demri and E. Orłowska, "Informational representability: Abstract models versus concrete models", in *Fuzzy Sets, Logics and Knowledge-Based Reasoning*, D. Dubois and H. Prade, Eds. Dordrecht: Kluwer, 1999, pp. 301–314.

Biographies and photographs of authors. A brief professional author's biography of up to 200 words and a photo of each author should be included with the manuscript.

Galley proofs. Authors should return proofs as a list of corrections as soon as possible. In other cases, the article will be proof-read against manuscript by the editor and printed without the author's corrections. Remarks to the errata should be provided within one week after receiving the offprint.

A copy of the JTIT is provided to each author of paper published.

Journal of Telecommunications and Information Technology has entered into an electronic licencing relationship with EBSCO Publishing, the world's most prolific aggregator of full text journals, magazines and other sources. The text of *Journal of Telecommunications and Information Technology* can be found on EBSCO Publishing's databases. For more information on EBSCO Publishing, please visit www.epnet.com.

(Contents Continued from Front Cover)

Editorial Office

National Institute
of Telecommunications
Szachowa st 1
04-894 Warsaw, Poland

tel. +48 22 512 81 83
fax: +48 22 512 84 00
e-mail: redakcja@itl.waw.pl
http://www.nit.eu

INSTYTUT ŁĄCZNOŚCI
PAŃSTWOWY INSTYTUT BADAWCZY