International Journal of Advances in Telecommunications Electrotechnics, Signals and Systems

a publication of the International Science and Engineering Society

Vol. 6, No. 1
2017

ISSN: 1805-5443

www.ijates.org

I J A T E S²

International Journal of Advances in Telecommunications Electrotechnics, Signals and Systems

a publication of the International Science and Engineering Society

Vol. 6, No. 1, 2017 ISSN: 1805-5443

Aims and Scope

The International Journal of Advances in Telecommunications, Electronics, Signals and Systems (IJATES²) is an all-electronic international scientific journal with the aim to bring the most recent and unpublished research and development results in the area of electronics to the scientific and technical societies, and is supported by the ISES (International Science and Engineering Society, o.s.). The journal's scope covers all the aspects of telecommunication, signal processing, theory and design of circuits and systems for electronics.

The IJATES² is ready to publish experimental and theoretical full papers and letters submitted by prospective authors. Paper submitted for publication must be written in English and must follow a prescribed format. All papers are subjected to a critical peer-review prior to publication.

The IJATES² is an open access journal which means that all content is freely available without charge to the user or his/her institution. Users are allowed to read, download, copy, distribute, print, search, or link to the full texts of the articles in this journal without asking prior permission from the publisher or the author. This journal provides immediate open access to its content on the principle that making research freely available to the public supports a greater global exchange of knowledge.

www.ijates.org

CONTENTS

Vol. 6, No. 1, 2017 ISSN: 1805-5443

Enterprise network with software Asterisk PBX based on the PLC technology

Michal Maar, Julia Sitarova and Milos Orgon

***Abstract*—This article presents the software Asterisk PBX solution design in enterprise PLC network (Power Line Communication). The description of the installation and configuration of software Asterisk PBX is involved in the design. The secure interconnection of two enterprise PLC network is implemented via the telecommunication tunnel with security grant using the Cisco routers. The connection between two Asterisk PBXs is designed in context of the establishment of the tunnel. The subject of the article is also cross/connection of exchanges Asterisk PBX and hardware PBX - IP Panasonic PBX K-NS500.**

***Keywords*—Asterisk PBX solution, PLC technology, IP Panasonic KX-NS500**

I. Introduction

VoIP (Voice over IP) technology has a number of advantages unlike public telecommunication network PSTN (Public Switched Telecommunication Network). The biggest advantage is cost savings when calling. Instead of paying telephone lines and circuits, customers pay only for the data connection. In addition, IP packets can be routed to any location with an Internet connection. As a part of the cost savings, employees can call in the enterprise network for free. Another advantage is the use of an existing network infrastructure, so it is no longer necessary to use the traditional telephone cables for interconnection of PBX. It is also possible configuration of the PBX from any location via the command line CLI or web interface. When communicating via VoIP because of additional cost savings for the company. VoIP technology is characterized by interoperability with older public telecommunication system PSTN. [1] In addition, voice in VoIP technology does not require high bandwidth (several kbit/s) and therefore is in the actual calls in corporate network, constructed based on PLC (Power Line Communication) technology which is described in [2-10], does not expect a significant reduction in quality of service. Therefore, PLC technology with low-cost software PBX Asterisk is suitable for the creation of a telecommunication platform for small and medium enterprise networks.

Manuscript received August 19, 2016, revised December 29, 2016.

This article is a part of research activities conducted at Slovak University of Technology Bratislava, Faculty of Electrical Engineering and Information Technology, Institute of Telecommunications, within the scope of the project KEGA No. 039STU-4/2013 “Utilization of Web-based Training and Learning Systems at the Development of New Educational Programs in the Area of Optical Transmission Media”.

M. Maar completed his studies at the Department of Telecommunications FEI STU Bratislava in July 2016, Slovakia. (e-mail: michal.maar@gmail.com).

J. Sitarova completed her studies at the Department of Telecommunications FEI STU Bratislava in July 2016, Slovakia. (e-mail: sitarovajulia@gmail.com).

M. Orgon is Associate Professor in the Institute of Telecommunications FEI STU in Bratislava, Ilkovičova 3, 81219 Bratislava, Slovakia,. (e-mail: orgon@ktl.elf.stuba.sk).

doi: 10.11601/ijates.v6i1.187

II. Softvare PBX Asterisk

PBX Asterisk is freely available software solution based on Linux. In addition to IP telephony, this PBX allows to use digital ISDN (Integrated Services Digital Network) and analog phones that are still in use in many companies. Asterisk also supports connectivity to the PSTN and other VoIP networks. Nowadays, the software PBX Asterisk has become a big competitor for traditional hardware PBX. One of the Asterisk advantages is the low cost for constructing PBX, whereas the PBX can be run on a personal computer or server. Another advantage is quick and easy installation and management over web interface control panel. Asterisk supports multiple protocols such as IAX, SIP, H.323 and MGCP. Asterisk solution is designed mainly for schools, hotels, small and medium-sized companies, where it's possible to call the flaps completely free. Asterisk provides a large number of services and functionalities. The most common include conference calls, forwarding, own numbering plan, voicemail, detailed information about each call, IVR, ACD, etc. [11]

The introduction of software PBX Asterisk in corporate environments has several advantages. Software PBX which is working on a more powerful PC or smaller server can convey up to several hundred calls. PBX advantage is that employees in the enterprise network can call each other for free.

A. Design and Implementation of Software PBX AsteriskNOW

In Fig. 1, there is an enterprise PLC network based on PLC technology, where was implemented design of software PBX. Enterprise PLC network consists of a ground floor and two floors. Floors are connected to each other by PLC technology, which uses the powerline communication in the building. Software and hardware IP phones, two switches, personal computers, router R-BA, printer and Wi-Fi router that provides connectivity for mobile phones with the application Zoiper are connected to the enterprise PLC network. Router R-BA is used to connect enterprise PLC network to external networks or Internet. Asterisk PBX which is running on a laptop is also implemented in enterprise network, too. Numbering and IP addressing plan

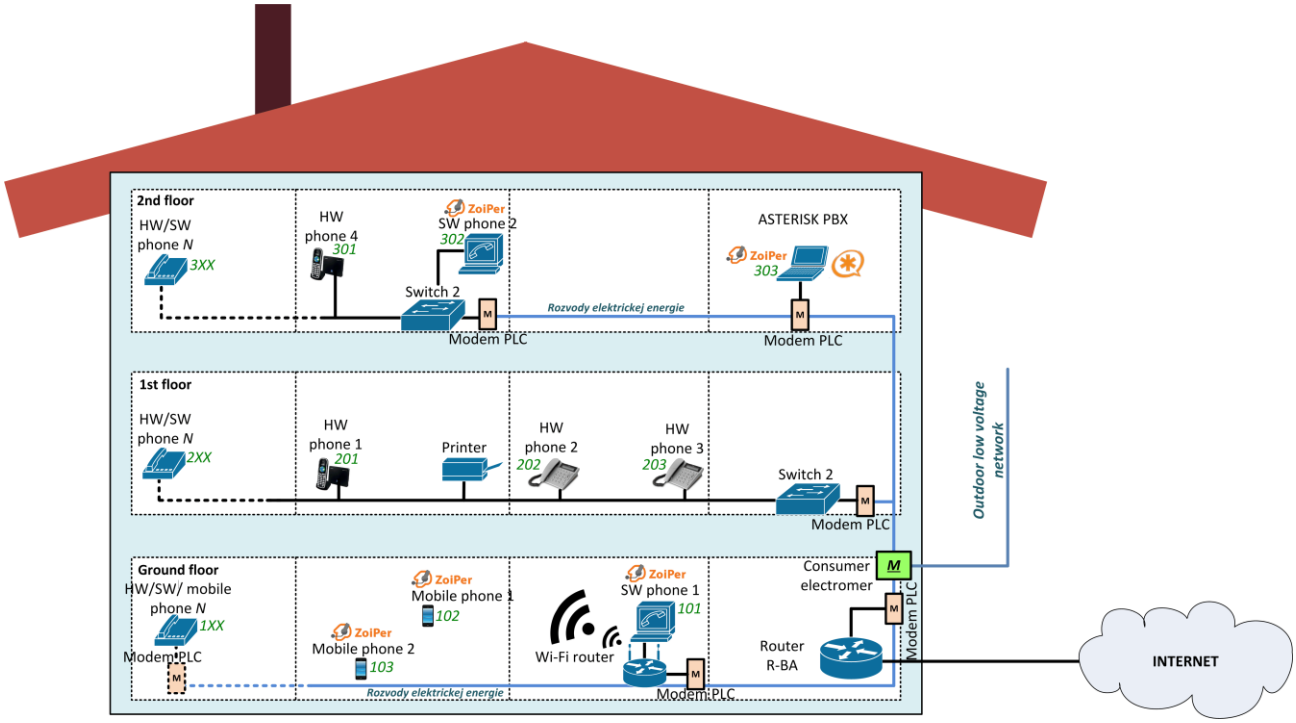


Fig. 1: Design of enterprise PLC network

TABLE I – Numbering and IP addressing plan

Floor	Extension number	Position	Device	Device IP address	PBX IP address
ground floor	101	Call center operator	SW phone	10.0.0.30/23	10.0.0.4/23
ground floor	102	Seller num.1	Mobile phone	10.0.0.31/23	10.0.0.4/23
ground floor	103	Seller num.2	Mobile phone	10.0.0.32/23	10.0.0.4/23
ground floor	1XX	New employee	SW/HW phone	10.0.0.33 - 10.0.0.130/23	10.0.0.4/23
1. floor	201	CEO	HW phone	10.0.0.131/23	10.0.0.4/23
1. floor	202	Accountant	HW phone	10.0.0.132/23	10.0.0.4/23
1. floor	203	Economist	HW phone	10.0.0.133/23	10.0.0.4/23
1. floor	2XX	New employee	SW/HW phone	10.0.0.134 - 10.0.0.230/23	10.0.0.4/23
2. floor	301	Programmer num.1	HW phone	10.0.1.1/23	10.0.0.4/23
2. floor	302	Programmer num.2	SW phone	10.0.1.2/23	10.0.0.4/23
2. floor	303	IT technician	SW phone	10.0.1.3/23	10.0.0.4/23
2. floor	3XX	New employee	SW/HW phone	10.0.1.4 - 10.0.1.100/23	10.0.0.4/23

are created to be able to connect up to 100 IP phones in each floor. Numbering and IP addressing plan are in Table I.

It was necessary to install virtualization tool Oracle VM VirtualBox to create a PBX Asterisk. VirtualBox can be used on your personal computer to run more virtual operating systems. In this case, the virtual PC serves like as a Asterisk PBX. Installation of Asterisk requires a relatively powerful computer to be able to deliver traffic for its original operating system, but also for virtual computer system. For that reason, CPU Intel Core i5-3210M, operating system Linux (type: Other Linux 64 bit) and three GB RAM were used to create a virtual server.

New virtual machine operating on the platform Linux in 64 bit version was created by the installed software VirtualBox. Than it was necessary to open AsteriskNOW.iso file which is freely available in the 32 or 64 bit version. During the installation, it was necessary to choose the network interface, with which it should Asterisk cooperate. In our case eth0 interface was used. In the next step it was necessary to specify TCP/IP settings and time zone, namely Slovakia/Bratislava. Finally, it was necessary to set the username and password in the Asterisk PBX. Access data are used for remote connections over SSL protocol.

After successful installation of Asterisk it was necessary to make a few configuration settings. In VirtualBox settings in created virtual machine AsteriskNOW, there was allowed network adapter and a type of connection was selected to bridge adapter. The network adapter and the type of connection to the bridged adapter was enabled in the network settings of the newly created virtual machine AsteriskNOW in VirtualBox. These settings are shown in Fig. 2. At next step, it was necessary to set the size of operational memory and number of processor cores that are used by Asterisk server. In the network settings it was necessary to set up sharing for VirtualBox access type. This setting allows to other network users to connect through a local computer connection. In the next step it was necessary to set up IP address from private ranges, in our case

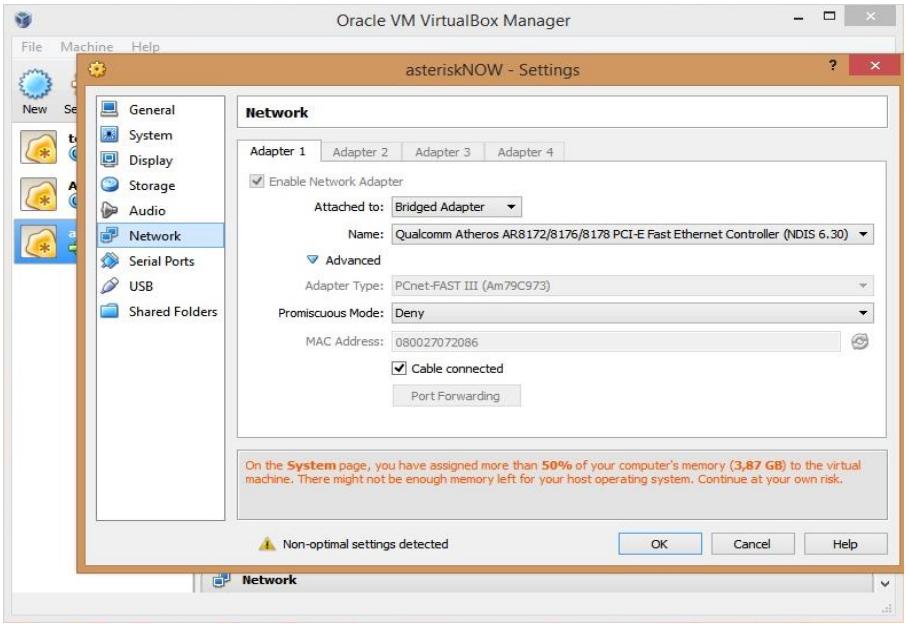


Fig. 2: Network settings

,,10.0.0.3", subnet mask ,,255.255.254.0" and preferred DNS server ,,10.0.0.1" on this type of access. As to communicate with other computers in created LAN, ethernet interface of the server has been set from the same IP address range, therefore ,,10.0.0.5" and subnet mask ,,255.255.254.0". In order to allow communication with other networks, was also necessary to set up the default gateway ,,10.0.0.1" on the router located on the edge of the network.

B. *AsteriskNOW Configuration*

In addition to the already mentioned settings it was necessary to create and customize other settings. Asterisk allows to manage through a web interface or the command line CLI. To access the command line you need to enter authentication credentials that were set during the installation. Because of its difficulty, Asterisk configuration over the command line interface CLI is mainly used by experienced administrators. Asterisk runs on the operating system Linux so network administrators use for management Linux commands. All files have the same syntax, but in each file are set various functions. The file structure looks like:

```
[section_title]
option=value.
```

After authentication, it was necessary to set general network settings like PBX IP address, subnet mask, network and default gateway. There settings are located in */etc/sysconfig/network-scripts/ifcfg-eth0* and their modification is possible with the *nano* Linux command. After installation, PBX IP address was obtained by DHCP protocol in the default configuration. But if we need static IP address of PBX then it would be necessary to change the *BOOTPROTO* value to *"none"*. It was necessary to set up:

```
  IPADDR="10.0.0.4"       ;      PBX      IP
address
  NETMASK="255.255.254.0"; subnet mask
  NETWORK="10.0.0.0"      ; network ID
  GATEWAY="10.0.0.1"      ;         default
gateway
```

After saving the Asterisk PBX it was necessary to restart computer using the command ,,service network restart". Asterisk IP address and config.d network settings can be verified by the command ,,ifconfig eth0". After these settings were Asterisk installed with the basic configuration, which was necessary for further work with PBX.

C. *Configuration by Web Interface*

Through a web browser and IP address of Asterisk PBX, which can be odtained from the command line of virtual PBX (Fig. 3).

D. *Creating Etensions*

Asterisk supports multiple protocols to create extensions, such as SIP, IAX2, DAHDi, etc. In this solution are used SIP extensions. First, you need to select an *Applications* and than *Extensions* item. In this way it is possible in the web interface to create, modify and delete extensions. When creating extensions, there are important parameters like *User Extension*, *Display Name* and *Secret*. Each modification in the management of Asterisk PBX must be confirmed by the *Apply Config* item.

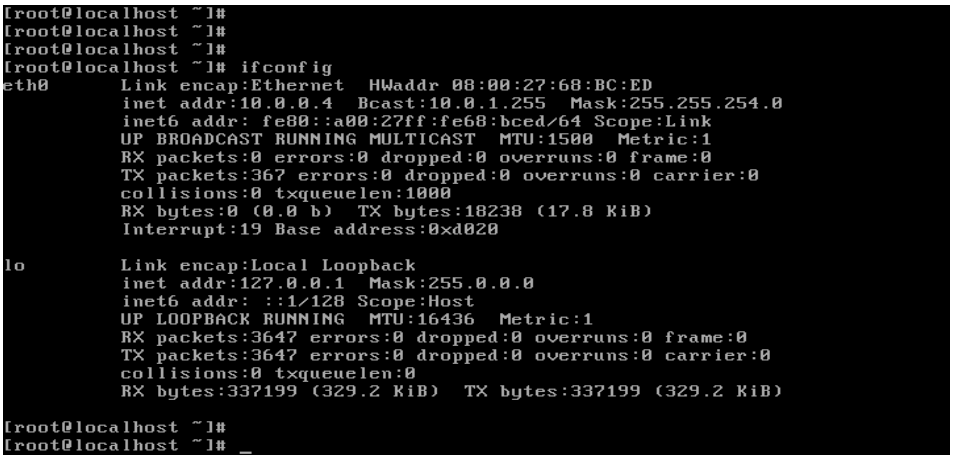


Fig. 3: Sample of Asterisk PBX command line

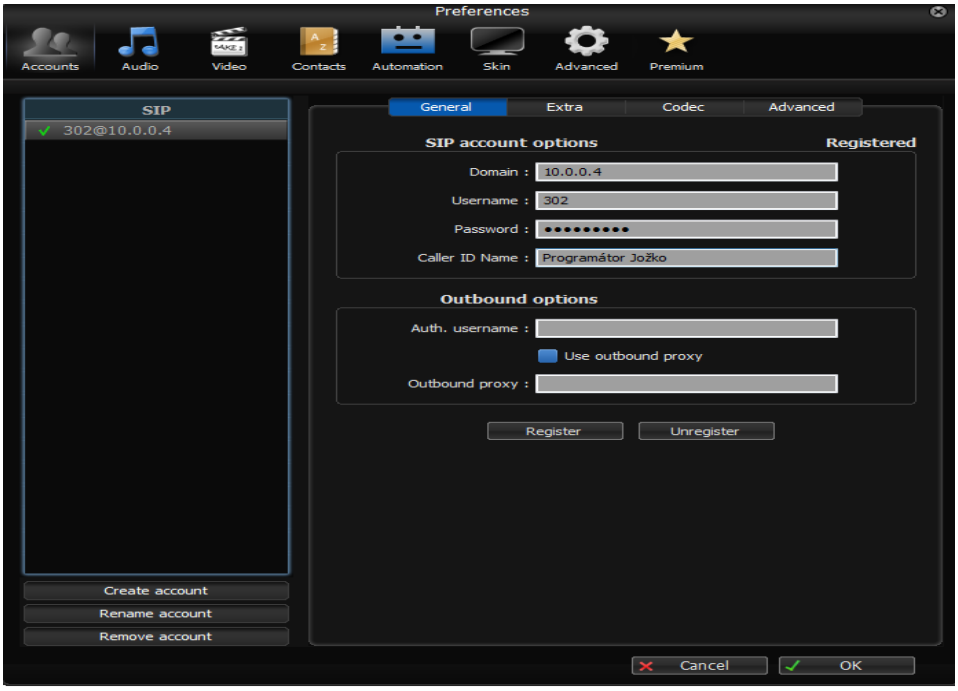


Fig. 4**:** Registered SIP extension

E. Hardware Phones Configuration

In this solution of Asterisk PBX in PLC network, there have been implemented hardware (Gigaset C470IP and Telco PH800N) and software (Zoiper) IP phones.

Wireless IP phone Gigaset C470IP can communicate with its base station up to 300 meters. It allows mixed telephony (PSTN and VoIP). Handset with ECO DECT technology reduces transmission power automatically. The transmission power is increased by distance - reduction of the transmitting power drops almost to zero if the handset is placed in dock station.

The advantage of softphones is a quick configuration and possibility to access the phone on a PC or a portable device such as a mobile phone or tablet. There are many applications that supports softphones. For our solution was selected frequently used software called Zoiper – free software with possibility of multiple voice and video codecs, which supports creation of multiple extension types like SIP, IAX, etc. Zoiper is also available for Android and iOS. Softphone is suitable for employees who work outdoors, such as sellers or managers.

When you create an extension using SIP software Zoiper, you must enter three important parameters: extension number, password and Asterisk PBX IP address. Fig. 4 shows the config.d and registered SIP extension.

III. Interconection of Two Corporate Networks Design for the Telecommunication Purposes

Telecommunication networks provide a wide range of opportunities to get new information, communicate and work over long distances. Demands on the quality of services are still increasing. Enterprises require not only fast, but also secure communication, both within one building or two buildings, but also between multiple remote offices often located abroad. Tunneling is used to satisfy the quality of these services, but also to increase safety. Tunneling is a process of transferring data from the local network A to the local network B over public network (e.g. Internet). After implementing site-to-site tunnel, sites can communicate just as if they were placed in the same segment. To prevent interception of communications, the connection between sites can be secured by encryption.

Telecommunication tunnels are mainly used in corporate networks to secure connection between two or more remote sites. In general, there are several tunneling protocols that differ from each other in implementation, possibility to use and security. The most common tunneling protocols are: GRE, IPsec, PPTP, L2TP, 6to4, SSH, etc. Some of these protocols has began to use in combination with another tunneling protocols due to their diverse functionality, for example pair GRE and IPsec or L2TP and IPsec. [12]

GRE (Generic Routing Encapsulation) was developed by Cisco and documented in RFC 2784. GRE creates a virtual point-to-point link between remote locations by Cisco routers over IP network. Through this protocol that operates at Layer 3 of RM OSI model, you can encapsulate wide variety types of packets to IP tunnel. Fig. 5 shows the structure of encapsulated packet. The advantage of GRE is to support unicast, broadcast and multicast transmission between multiple sites and also GRE allows to transmit static and dynamic routing protocols such as RIP, OSPF, etc. In fact, other tunneling protocols are not able to provide this functionality so the GRE is irreplaceable. [13].

Fig. 5: The structure of encapsulated packet

IPsec (Internet Protocol Security) is an IETF standard that defines how to safely access to a virtual private networks and also provides secure IP packets transmission. IPsec works at Layer 3 of RM OSI model in two modes: transport and tunneling mode. It is implementable with IPv4 and IPv6 protocol. However, IPsec cannot encapsulate packets and routing protocols. For this reason, functionality of protocol GRE is very elegantly combines with safety of protocol IPsec. Universal tunnel GRE is placed inside a secure tunnel IPsec, as you can see in Fig. 6.

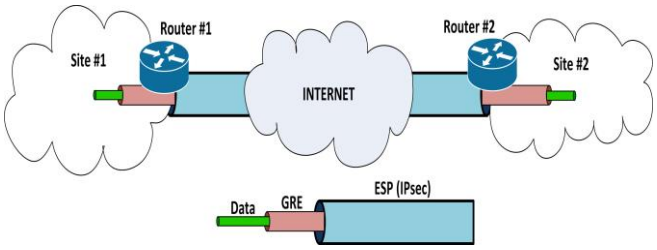


Fig. 6: GRE over IPsec

A. Interconnection of Two Sites by GRE over IPsec Protocol

The network design was designed for the company with office in Bratislava, assuming expansion to the Thorn city (opening branch in Poland). The new office in Poland was necessary to connect with the office in Bratislava. Those two connected sites should have to act like being in single segment of enterprise network. A very important requirement was the security of data transfer between these sites. Creating a GRE tunnel and subsequent security through IPsec ensuring, respectively, use the GRE over IPsec protocol, seemed to as to be the most ideal way to connect these sites.

The tunnel through GRE protocol can be formed between routers placed in the edges of two local area networks. The Cisco 1841 routers with operating system IOS version 12.4 were used for these purposes. The GRE tunnels with IPsec protocols are supported by the routers mentioned above. License package *securityk9* need to be installed and activated for support of security protocols in newer versions of operating system IOS (version 15 and upper).

Cisco ISR 1841 are modular routers with LAN and WAN interfaces. Routers provide basic features, such as linking multiple computer networks, security, fast and high quality service transmission for small to medium sized enterprises. Cisco routers contain flash memory the most common of 64 MB, AUX port, USB port, console port, two serial ports and two FastEthernet ports. You can buy additional modules, which allow expansion of port capacity.

Cisco ISR 1841 routers have been configured by free software PuTTY. PuTTY is used as a client SSH, Telnet, Rlogin and is also used for a serial COM port connections. At first configuration router used COM port - it is possible to manage the Cisco router through console and command line after connecting the router's console port with PC's COM port. The computer network was formed to create a connection between two remote areas as is shown in fig. 7. Router ISP serves as a simulation of the Internet, because the left and right side of the router ISP are networks with public IP address range. R-BA and R-TO routers are on the edge of the networks and provide routing between sites. Between R-BA and R-TO was created GRE over IPsec tunnel.

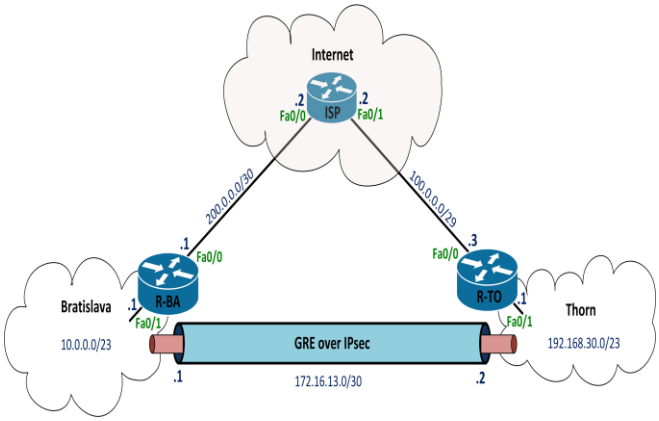


Fig. 7: Connection of two remote locations design via Cisco routers

Routers R-BA and R-TO were config.d as follows:

1) The router was renamed from the original name „Router“ to „R-BA“ and at the interfaces FastEthernet 0/0 and 0/1 have been set up IP addresses, like in Fig. 7. Each interface has been enabled by command „`noshutdown`“.

   The router was renamed from the original name „Router“ to „R-BA“ and at the interfaces FastEthernet 0/0 and 0/1 have been set up IP addresses, like in Fig. 9. Each interface has been enabled by command

„noshutdown“:

```
Router#configure terminal
Router(config)#hostname R-BA
R-BA(config)#interface fa0/0
R-BA(config-if)#ip address 200.0.0.1
255.255.255.252
R-BA(config-if)#no shutdown
R-BA(config-if)#exit
R-BA(config)#interface fa0/1
R-BA(config-if)#ip address 10.0.0.1
255.255.254.0
R-BA(config-if)#no shutdown
R-BA(config-if)#exit
```

2) Static routing through an ISP router due to interconnection of routers R-BA and R-TO was set by the following command:

```
R-BA(config-if)#ip route 100.0.0.3
255.255.255.255 200.0.0.2
```

3) Between routers R-BA and R-TO, GRE tunnel has been created by virtual interface called „tunnel 1“. Tunneling mode was used and set to GRE. Source IP address which is located at the interface FastEthernet 0/0 was specified by the command „source“. Subsequently, the destination IP address was specified by the command „destination“. Then, on R-BA router was set start IP address „172.16.13.1“ and on the router R-TO end IP address „172.16.13.2“ of the tunnel. These two IP addresses must be on the same subnet, in this case „255.255.255.252“. Finally, the dynamic routing protocol OSPF was applied, which will be transmitted by GRE tunnel. OSPF requires the IP address of the neighbor network, wildcard mask and set the area. In this case was set area 0. Depending on the configuration of the router R-BA, router R-TO is config.d analogically:

```
R-BA#configure terminal
R-BA(config)#interface tunnel 1
R-BA(config-if)#tunnel mode gre ip
R-BA(config-if)#tunnel source
fastEthernet 0/0
R-BA(config-if)#tunnel destination
100.0.0.3
R-BA(config-if)#ip address 172.16.13.1
255.255.255.252
R-BA(config-if)#router ospf 1
R-BA(config-router)#network 172.16.13.0
0.0.0.3 area 0
R-BA(config-router)#network 10.0.0.0
0.0.1.255 area 0
```

4) To verify the configuration, it is possible to use several commands, for example ,,show ip interface brief | include Tunnel", ,,show interface Tunnel 1" or ,,show ip route ospf".

5) In this part of the configuration was created GRE tunnel between two routers, if you like between LAN networks in Bratislava and Thorn. Communication over GRE tunnel is not encrypted. To secure communication between sites, GRE was placed into IPsec tunnel. Then it was necessary to create ISAKMP policy on R-BA. In ISAKMP policy AES encryption algorithm, authentication with shared password, Diffie-Hellman group 2 and lifetime 3600 seconds were set. The configuration was repeated analogically on the router R-TO and finally was set on both routers shared key „PASS“ with the IP address of the remote neighbor:

```
R-BA(config)#crypto isakmp policy 10
R-BA(config-isakmp)#encryption aes 256
R-BA(config-isakmp)#authentication pre-
share
R-BA(config-isakmp)#group 2
R-BA(config-isakmp)#lifetime 3600
R-BA(config)#crypto isakmp key PASS
address 100.0.0.3
```

6) In the next step there was created transform set, in which was set IPsec to transport mode. Using AH or ESP protocols, encryption standard AES with key length of 256 bits and hash algorithm HMAC-SHMA were defined in the created set of transformation named TRANS. This transform set was analogacally set on the router R-TO:

```
R-BA(config)#crypto ipsec transform-set
TRANS esp-aes 256 esp-sha-hmac
R-BA(config-if)#mode transport
```

7) The next step was to create encrypted map named MYMAP. The map contains the definition of neighbor (100.0.0.3), link to transform set TRANS and *access list 100*. Access lists define packets which will be encrypted by crypto map. By using the list of *access list 100* is permitted all GRE traffic which is not blocked. Crypto map and access list was created analogically on R-TO router:

```
R-BA(config)#crypto map MYMAP 10 ipsec-
isakmp
R-BA(config-crypto-map)#set peer
100.0.0.3
R-BA(config-crypto-map)#set transform-
set TRANS
R-BA(config-crypto-map)#match address
100
R-BA(config)#access-list 100 permit gre
any any
```

8) The last step was the activation of crypto map. The map refers to the interface that serves as the end point of the tunnel.

```
R-BA(config)#interface fastEthernet 0/0
R-BA(config-if)#crypto map MYMAP
```

```
R-BA#show crypto session
Crypto session current status

Interface: FastEthernet0/0
Session status: UP-ACTIVE
Peer: 100.0.0.3 port 500
  IKE SA: local 200.0.0.1/500 remote 100.0.0.3/500 Active
  IPSEC FLOW: permit 47 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
        Active SAs: 2, origin: crypto map
```

Fig. 8: Verify the encryption functionality

There are several ways to verify the functionality of the GRE tunnel encryption. Probably the quickest way is a listing of command „`show crypto session`“, which is shown in Fig. 8.

All data that are transmitted between the routers R-BA and R-TO with the public IP addresses at the network edge are encrypted. The traffic between routers R-BA and R-TO was captured using the PC with software Wireshark which was placed to the connection between the routers. Fig. 9 shows encapsulated packets using the protocol ESP.

Communication between two sites has been provided by GRE over IPsec. This allowed that employees can securely send internal data to each other.

B. Interconnection of Two Asterisk PBXs by IAX Protocol

The introduction of two Asterisk PBXs and their interconnection through trunk allows a reduction in load of the link, redundancy and prevention against outages. For two sites (A and B) it is preferred to have one branch PBX for each site. Calls in each site (A and B) runs through internal PBX and in the event of connection loss between sites A and B, employees in site B can communicate between each other. If the PBX is only in the site A and all users from the site B would be connected to PBX from site A, as in the case of connection loss between site A and B, you wouldn't make calls between employees in the site B. Some enterprises, such as factories, cannot afford these failures. The advantage of introducing PBX in each of the sites is redundancy. In the case of outage PBX in the site A, the employee IP phones can connect to the PBX in site B and thus continue in the communication.

Interconnection of PBXs is often established via protocol SIP or IAX2 in practice. The advantage of SIP trunk is easier error detection, which are in the form of text messages. In IAX2 trunk are error messages in binary form. On the other hand, the advantage of IAX2 trunk is configuration simplicity when connecting two PBXs, which are located in other networks. SIP trunk is more difficult to config.d if PBXs are located in other networks.

After secure interconnection of sites in Bratislava and Thorn using routers R-BA and R-TO, employees can share internal data and communicate with each other. The interconnection of two software PBXs using IAX2 protocol was designed and implemented for reasons of redundancy and to save the bandwidth. Interconnection configuration of two software PBXs is shown in Fig. 10.

TABLE 2: IAX2 trunk parameters

Parameter:	**Value:**	**Note:**
Trunk Name:	To Thorn_iax	Trunk name
Outbound CallerID:	Call from Bratislava	Name, which is displayed on the phone to user in Thorn
Dialed Number Manipulation Rules:	8XX 9XX	Extension ranges in Thorn (800-899 and 900-999)
Peer details:	host=192.168.30.4 username=thorn secret=passtrunk type=peer qualify=yes context=from-internal trunk=yes	IP address of PABX, on which heads trunk (in Thorn) named: *thorn* and password: *passtrunk*
User Context ID:	Bratislava	Account name associated with the parameter User Details
User Details:	secret=passtrunk type=user host=192.168.30.4 context=from-trunk	Connection parameters (trunk)

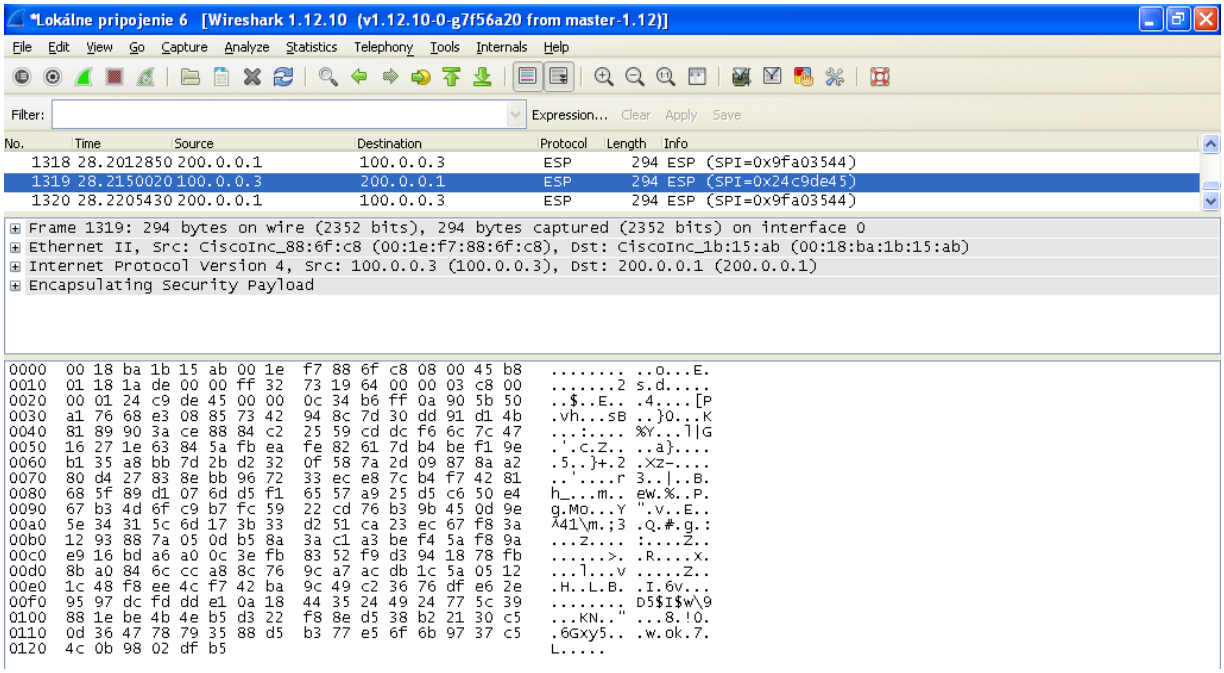


Fig. 9 - Packets captured between two locations

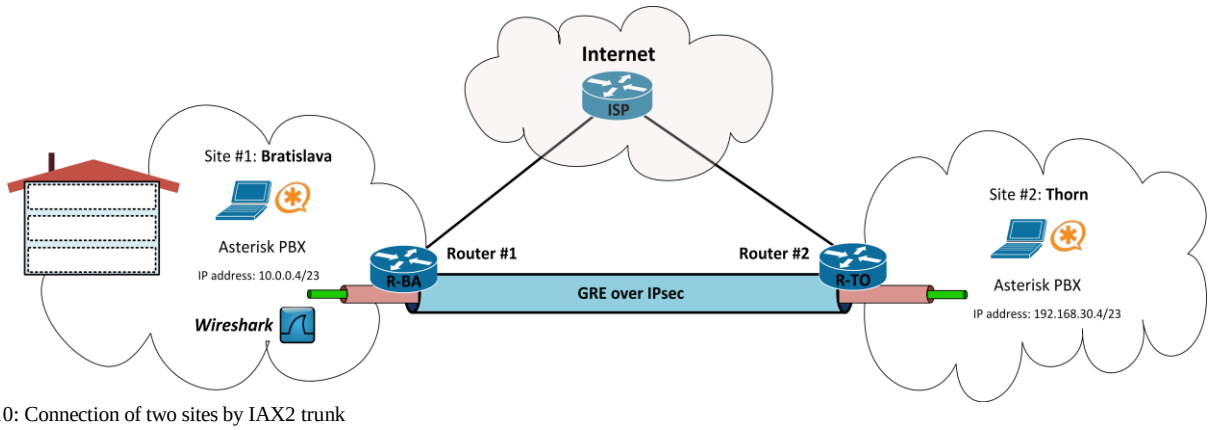


Fig. 10: Connection of two sites by IAX2 trunk

IAX2 trunk configuration between two Asterisks consists of three basic steps: trunk configuration, inbound and outbound routes. It is necessary to configure both Asterisks analogically. The following procedure describes how to config. Asterisk PBX in Bratislava part.

It is necessary in the management of PBX Asterisk select *Trunks* button. To interconnect of Asterisk PBXs in this design was selected IAX2 protocol, and it was necessary to set the following parameters (Table 2).

The second step was configuring of outbound route, then was created new outbound route named *ThornExt_iax* and the following parameters was set (Table 3).

TABLE 3: Outbound route parameters *ThornExt_iax*

Parameter:	**Value:**	**Note:**
Route Name:	ThornExt_iax	Outbound route name
Dial Petterns that will use this Route:	8XX 9XX	Extension range in Thorn (800-899 and 900-999)
Trunk Sequence for Matched Routes:	To Thorn_iax	Trunk with which will outbound route cooperate

Finally, it was created Inbound route named *From_Thorn_iax*. In the Inbound route it was necessary to create *Ring Groupe*. When creating a ring group, it has been set it's number, a list of all extensions and destination extension required in case of problems. After configuration of all required parameters for Asterisk PBX in Bratislava it was necessary to config. Asterisk PBX analogically in Thorn.

To verify IAX2 trunk between PBX's the Wireshark software was used. It was possible to watch the communication between PBX's by Wireshark. A computer with installed software Wireshark was placed between the R-BA router and Asterisk PBX in Bratislava. Fig. 11 shows captured communication of VoIP call between PBX's in Bratislava (IP 10.0.0.4/23) and Thorn (IP 192.168.30.4/23).

The call was processed from the extension 101 in Bratislava to extension 805 in Thorn. Asterisk PBX web interface enables a several functions. One of them is monitoring of every activity of PBX, known as LogFiles. Fig. 12 illustrates the process of dial an extension 805 in Thorn from extension 101 located in Bratislava. This log in the Fig. 12 shows successfull establish of connection between two software PBXs in Bratislava and Thorn.

C. Interconnection Design of Two PBXs via MPLS Network

The telecommunication infrastructure design was designed for the company that founded another office in Slovakia (in the Poprad city). The office disposed of IP Panasonic PBX KX-NS500, the PLC backbone communication network composed of ZyXEL PLA5206 modems with transfer speed up to 1000 Mbps. The IP Panasonic PBX had also an extension module KX-NS520 that allows you to connect a larger number of telephones. Therefore, it was necessary to resolve interconnection of hardware PBX Panasonic KX-NS500 with software Asterisk PBX in Bratislava additionally.

PLC modem ZyXEL PLA5206 is one of the newest products of PLC technology, which is based on the HomePlug AV2 standard and is also compatible with previous standards. This modem provides a theoretical bit rate up to 1000 Mbit/s. Modem operates in the frequency range from 2 to 86 MHz and has the function of QoS support, which is important in VoIP voice services. These new modems are much easier to use than the older one. It is necessary to connect PLC modems to the power lines and also to the devices. Then the communication between these devices can be established. Management via web interface is not needed, because the modems are automatically paired. Secure communication using AES encryption with a key length of 128 bits is automatically established too.

The Panasonic PBX KX-NS500 creates an intelligent hybrid IP communications system designed for small and medium-sized businesses which is easily configurable and expandable according to the needs of the business. The PBX supports to connect many different types of terminals – analogue, digital phones, SIP software and IP telephones. The advantage in economic terms is the ability of using analogue and digital telephone. As a result, reuse of an older communication system of the company is possible. The PBX provides many helpful features that can simplify the communication of the company – for example call centers which CTI server function is not needed, or Unified Communications function. The PBX provides recording and backup of conversations in relation to improving the communications services of company using statistics and analysis of customer calls. The PBX is managed through a

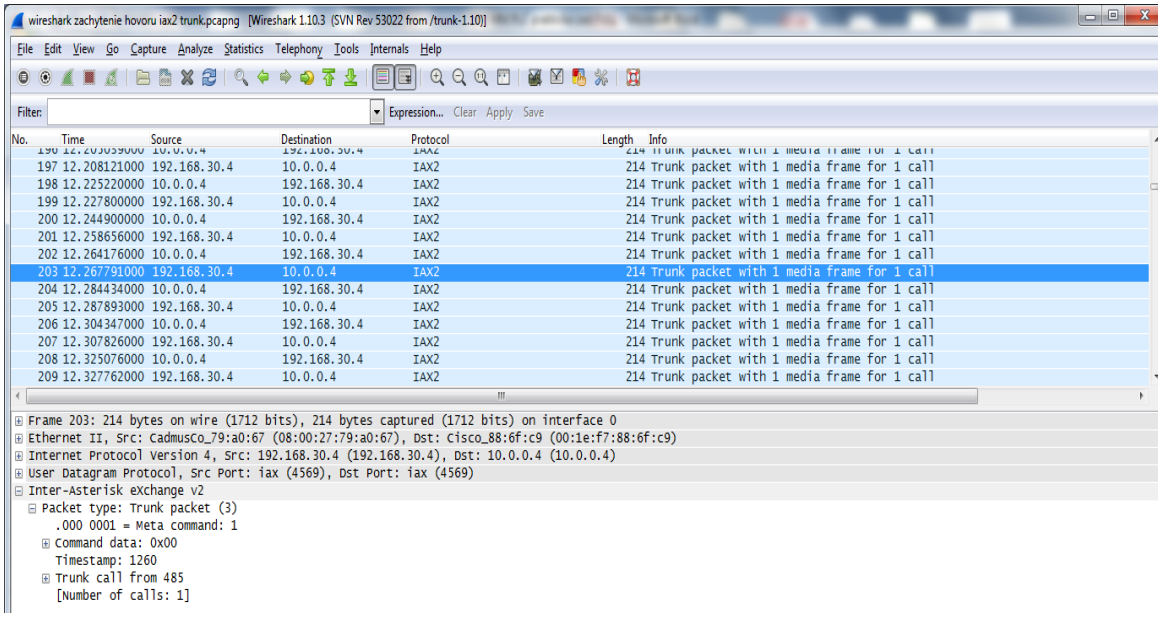


Fig. 11: Captured communication between two Asterisk PBXs

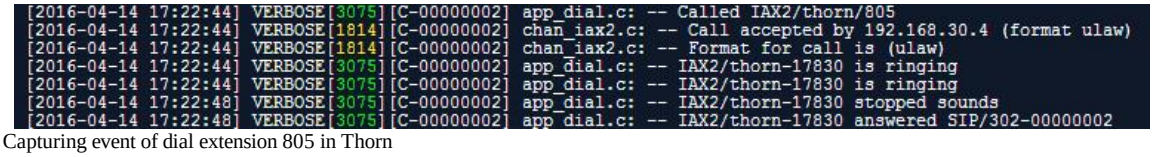


Fig. 12: Capturing event of dial extension 805 in Thorn

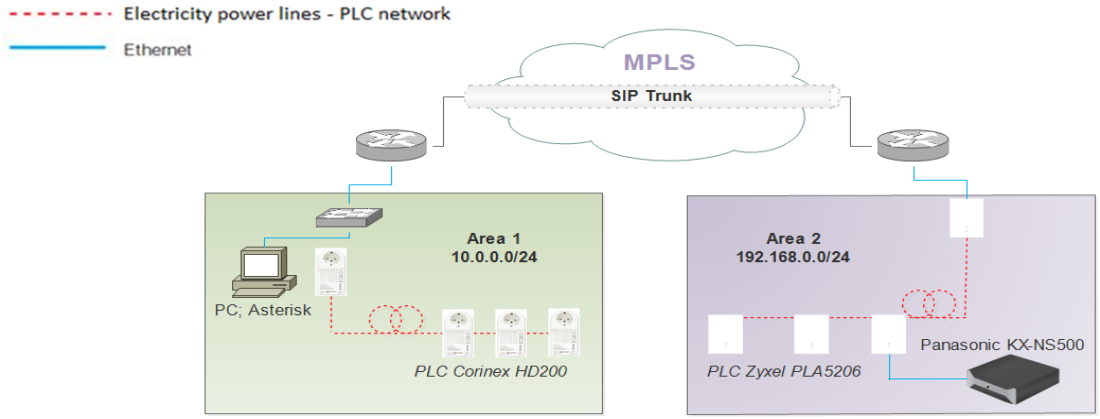


Fig. 13 Interconnection of PBXs via MPLS network

web interface, where all the PBX`s settings can be config.d and managed.

The designed scheme of interconnection between two segments of enterprise network is shown in Fig. 13. The first segment was served by Asterisk PBX and the second segment was served by hardware Panasonic PBX KX-NS500.

In previous section the design and forming of LANs in Bratislava and Poprad were described in detail. At this stage the networks were ready for interconnection. It would be necessary to use a provider`s network to connect the sites via MPLS network. The network design involves this way of interconnection due to its reliability, speed and security. MPLS network is set of switches or routers that switch all the packets according to their tag. The tag is added to each packet at the entrance of the network. As a result of simplicity, the transfer speed of the packets is higher because the packets are not routed with complex logic – packets are simply switched. Considering the VoIP traffic in our design, we had to select the reliable, fast and QoS providing connection. The MPLS network has all of mentioned requirements – apart of its speed it is a very stable network because of the simple switching logic. Cable length between computers or PLC modems was the order of several meters. The QoS guarantee is related to ability of assigning different levels of priority to each packet in MPLS network. Considering these reasons, use of the MPLS network in the design was selected.

Finally, only the logical connection between software Asterisk PBX and hardware Panasonic PBX KXNS500 via SIP Trunk was implemented due to economical reasons. However, this solution is a subject of another article because of the scope of this article.

IV. Conclusion

The purpose of the article was the software Asterisk PBX solution design in enterprise PLC network. The description

of the installation and configuration of software Asterisk PBX was involved in the design. The secure interconnection of two enterprise PLC network was implemented via the telecommunication tunnel with security grant using the Cisco routers. In final part, the connection between two Asterisk PBXs was designed in context of the establishment of the tunnel. A part of the design was the design of connection with hardware IP Panasonic PBX K-NS500.

REFERENCES

[1] B. Hartpence, *Packet Guide to Voice over IP*, O'Reilly Media Inc., www.it-ebooks.info, Twitter: 2oreillymedia facebook.com/oreilly, Published by O´Reilly, Media, Inc. 1005 Gravenstein High North, Sebastopol, CA 95472, 2013, ISBN 978-1-449-33967-8

[2] M. Orgon, R. Roka, and J. Misurec,: *Smart Grid and Power Line Communication***,** Publishing STU Bratislava, 396 pages, 2015, ISBN 978-80-227-4356-3.

[3] J. Misurec and M. Orgon, Modeling of Power Line Transfer of Data for Computer Simulation, *Int. J. Communication Networks and Information Security (IJCNIS)* Vol. 3, No. 2, 2011, pp. 104-111, Pakistan, ISSN 2073-607X,

[4] M. Orgon and I. Bestak, Performance Measurement of Encryption Algorithms used in PLC Devices, *Int. J. of Research and Reviews in Computer Science*. Vol. 2, No. 5, 2011, pp. 1218-1221, ISSN 2079-2557.

[5] S. Klucik, J. Taraba, M. Orgon, and D. Adamko, The Use of PLC Technology in Broadband Services Offered to Households, *Int. J. of Information and Computer Science (IJICTS)*, 2012, 4, pp. 1-8, ISSN: 2074-9007 (Print), ISSN: 2074-9015 (Online), MECS Publisher (http://www.mecs-press.org/), DOI 10.5815/ijicts.2012.04.01

[6] I. Bestak and M. Orgon, The use of encryption algorithms in PLC networks, *Int. J. of Information Technology and Business Management (IJTBM & ARF)*, Vol. 13, No. 1, May 2013, ISSN 2304-0777,

[7] M. Orgon, I. Bestak, M. Halas, and A. Kovac, Finding the best encryption algorithms for PLC technology, in *Proc. Knowledge in Telecommunication Technologies and Optics - KTTO 2011*, Szczyrk, Poland, pp.. 152-156- ISBN 978-80-248-2399-7,

[8] J. Misurec and O. Orgon, The Cascade Models for Simulation of PLC Communication, in *Proc. 6th Int. Conf. Teleinformatics - ICT 2011*, Brno, 2011, pp. 53-56- ISBN 978-80-214-4231-3,

[9] M. Halas, I. Bestak, M. Orgon, and A. Kovac, Performance Measurement of Encryption Algorithms and their Effect on Real Running in PLC Networks,

[10] F. Hossner, J. Hallon, M. Orgon, and R. Roka, Software PBX Asterisk platform designed for PLC, *Int. J. Engineering Reearch & Technology (IJERT)*, Vol. 5, No. 01, January 2016, ISSN: 2278-0181,

[11] M. Voznak, Telephone exchanges Asterisk, *Theory and Practice of IP telephony 3*, the two-day expert seminar, Convention Cente, Hotel Olšanka, 5 and 6 November 2008

[12] D. Adam, M. Gemeranova, L. Marsik, and P. Sucha, *Tunneling*, Comenius University in Bratislava, Faculty of Mathematics, Physics and Informations, lecture notes, Bratislava, Slovakia

[13] Cisco Networking Academy, *CCNA4 Routing and Switching, Connecting to Networks, Securing Site-to-Site* (Module 7), <www.netacad.com>

Michal Maar was born in Bratislava, Slovakia, in 1992. He received the B.E. and M.E. degrees in Faculty of Electrical Engineering and Information Technology of Slovak University of Technology (FEI STU) Bratislava in 2014 and 2016, respectively. He currently works in the field of traffic safety telecommunications networks.

Julia Sitarova was born in Bratislava, Slovakia, in 1992. She received the B.E. and M.E. degrees in Faculty of Electrical Engineering and Information Technology of Slovak University of Technology (FEI STU) Bratislava in 2014 and 2016, respectively. She is currently working on the design of optical networks.

Milos Orgon was born in Piestany, Slovakia, in 1956. He received the Master degree and PhD degree in the Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava in 1980 and 1988, respectively. Nowadays he works as an assistant professor at the Department of Telecommunications of FEI STU Bratislava. He has been engaged in research and development of telecommunication networks and services in liberalized environment for area of convergent technologies. At present he is currently engaged in research on the optimal design of networks and technological components, implementation of functions, services and applications and data security in projects KEGA No. 039STU-4/2013 “Utilization of Web-based Training and Learning Systems at the Development of New Educational Programs in the Area of Optical Transmission Media”.

ICMP-based Third-Party Estimation of Cloud Availability

Maurizio Naldi

***Abstract*—Cloud availability is an important parameter present in a typical Service Level Agreement (SLA). In order to check compliance with SLA commitments, a third party availability measurement is strongly needed. An availability estimation methods is evaluated here, based on the periodic repetition of sequence of probing packets in ICMP. Majority Voting, which declares a cloud to be available only if a majority of probing packets gets an echo from the cloud, appears to provide an accurate estimation even when the packet loss probability is rather high.**

***Keywords*—Cloud, Availability, ICMP, Service Level Agreement (SLA).**

I. Introduction

Cloud availability is a major performance parameter for cloud platforms. When an individual or a company switch to the cloud, they wish the platform to be at least as available as their in-house infrastructure. For that reason, availability is always present among the parameters to be monitored in cloud monitoring systems [1] and to be considered in cloud platform assessment systems [2], [3]. All major commercial cloud platforms typically include it in SLAs [4], [5], and boast of their values: in the survey reported in [6], 15 providers out of 17 declared at least 99.9% availability, with 12 providers declaring 100% availability.

In order to check such performance claims, third-party availability measurements are strongly desired. While a model to predict cloud reliability has been proposed in [7], and the availability of single servers has been analysed in [8], not many efforts are present in the literature to investigate the overall availability actually offered on commercial platforms. For example, availability is not considered in the comparison carried out in [9]. In the description of a major commercial platform, Microsoft Azure, provided in [10], though a high availability is claimed right in the title, no figures are provided for the expected availability. Notable exceptions are represented by [11] and [12], where a probing method based on ICMP (Internet Control Message Protocol), suitable for third-party measurements, is adopted, though exhibiting several criticalities [13]. A different approach relies on reported data rather than actual measurements: data from cloud provider status dashboards and press releases have been collected and analysed in [14] and [15].

In this paper we investigate the accuracy of the ICMP-bsaed approach to measure the availability of a cloud, after the early analysis reported in [16]. Building on the impact of networking failures on the estimation of availability as evaluated in [16], we provide a MonteCarlo simulation-based estimation of the availability achieved under concurrent true cloud outages and networking failures. Three different criteria to output an availability statement are compared: Majority voting, Unanimous Positive voting, and Unanimous Negative voting. We find that Majority Voting provides an accurate availability estimation in a wide range of cases, while the other criteria err on either side, with heavy underestimation when the packet loss probability exceeds 10^{-3}.

The paper is organized as follows. In Section II we describe the testing arrangement based on ICMP, while its performances are analysed in Sections III, IV, and V on three different timescales.

Manuscript received October 30, 2016, revised January 27, 2017.

M. Naldi is with the Department of Computer Science and Civil Engineering, University of Rome Tor Vergata, 00133 Roma, Italy e-mail: maurizio.naldi@uniroma2.it.

This research has been supported by the Italian Ministry of Education, University, and Research (MIUR) under PRIN 2012C4E3KT national research project "AMANDA Algorithmics for MAssive and Networked DAta".

II. Testing Methodology

The way we measure availability has a great impact on the numeric value we get. In this section, we clarify what is meant by availability in this context and how we measure it by using ICMP.

The availability A of a system, which undergoes phases of normal working separated by outages, is defined as the ratio of the uptime and the total time:

$$A = \frac{\text{Uptime}}{\text{Total Time}} = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}}. \quad (1)$$

In the context of a cloud, since the service provided by a cloud is to respond to service demands, such as for some content stored in the cloud (cloud storage) or for the result of some processing task carried out on the cloud (cloud computing), we can consider as uptime the time during which the cloud responds, and as downtime the time during which it stops doing so.

It is therefore natural to see the cloud as oscillating between two states: UP and DOWN. This is called the *Dual State model* in [17], where transitions between the two states are triggered by failures and service demands are not satisfied throughout the downtime period. Several real world examples of Service Level Agreements in clouds are amenable to being formulated according to this model, e.g., Amazon EC2, HP Cloud Compute, and Google Apps SLA, again as observed in [17]. It is implicit that this model considers no graceful degradation: either the cloud responds to the service demand or not.

In order to check whether the cloud is up or down, the method we analyse here, proposed in [12], employs the *ping* command of the Internet Control Message Protocol (ICMP)

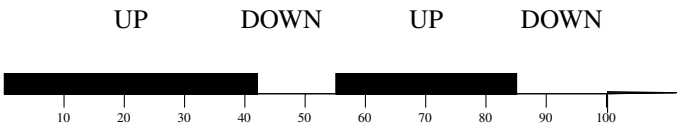


Fig. 1. Sequence of up and down states

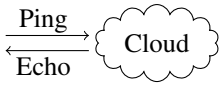


Fig. 2. Testing arrangement

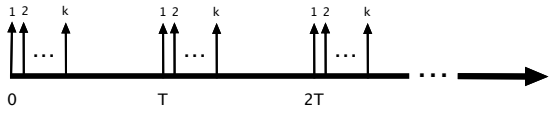


Fig. 3. Test sequence

[18]. A ping-based approach to measure availability had already been employed in [19] to analyse cloud storage facilities and in [20] to analyse the reliability of internet sites. The method operates by sending echo request packets (*pings*) to the target cloud (the front-end server, e.g., the hostname in the URL of the stored object for cloud storage) and counting the echoes as a measure of success. A ping response indicates that the target host is connected to the network, is reachable from the query agent, and is in a sufficiently functional state to respond to the ping packet. After waiting for ICMP echo replies, the protocol reports packet loss and round-trip-time statistics. Though it is recognized that failure to respond is not so informative because it cannot be reliably inferred that the target host is not available, the foremost causes of failed response are related to the network (and are accounted for in our analysis later), excepting the presence of some form of firewall in the end-to-end path that blocks the ICMP packet being delivered [21].

Under this approach, the cloud is seen as a black box (see Fig. 2). Though the resource may be located elsewhere, so that queries are actually served by a server in a different location, the availability of the cloud is embodied by the responsiveness of the front-end server. Therefore, this scheme serves equally well as a model to analyse configurations where contents or processing resources are distributed over several geographical areas, as long as the service access point is one.

Each ping allows therefore to see if the front-end server is up and running. Pings are not shot in isolation, but are sent off in bursts to achieve a better accuracy in the face of temporary glitches. As shown in Fig. 3, the tester sends off a burst of k pings (in [12] a repetition period of 2 seconds was envisaged), and the whole sequence is periodically repeated every T seconds (which, again in [12], was set at 10 or 11 minutes). If the aim is to compare the observed availability against the Service Level Agreement commitments over any period of length C, we consider an observation window of length C for contractual purposes.

At the end of each probing sequence made of k pings, the tester outputs an availability statement concerning the cloud, declaring the cloud service either available or not. That statement is kept as valid till the next probing sequence, when a new availability statement is emitted. The observation window can therefore be considered as made of $B = \lfloor C/T \rfloor$ time blocks, so that we can have a number of availability statements in the $[0, B]$ range, where the lowest value (0) represents a service considered as totally unavailable over the observation window, while the largest value (B) represents a 100% availability. If we use the symbol N_{out} to indicate the number of blocks for which a NOT AVAILABLE statement is output, the availability estimate is:

$$\hat{A} = 1 - \frac{N_{\text{out}}}{B} = 1 - \frac{N_{\text{out}}}{\lfloor C/T \rfloor}. \tag{2}$$

In order to correctly estimate large availability figures, the number of blocks must be correspondingly large, otherwise the granularity due to the blocks will mask short unavailability periods. For example, if $B = 100$, the next largest availability figure to 100% that we can estimate is $99/100 = 0.99$, i.e. just a 2-nine availability. If we wish to measure availability figures as large as four nines ($A = 0.9999$), the minimum number of blocks must be 10000. In order to achieve that number, if we set $T = 10$ minutes, the observation window must be at least $10 \cdot 10000 = 100000$ minutes long, which corresponds to slightly more than 69 days. In general, to measure an availability A, the observation window must be

$$C \geq \frac{T}{1 - A}. \tag{3}$$

In order to arrive at an availability statement for any single sequence of k pings, we consider three alternative criteria, by adding a Unanimous Positive voting to the two listed in [16]:

- Majority voting
- Unanimous Positive voting
- Unanimous Negative voting

In Majority Voting an outage is declared if a majority of pings get no echoes. In Unanimous Positive voting, all echoes must be received to declare the cloud available. In Unanimous Negative voting, an outage is instead declared if no ping gets an echo. What we get in an example for sequences made of $k = 5$ pings is shown in Table I. As can be seen, the Unanimous Positive voting criterion will lead to the most severe availability statements, while the Unanimous Negative voting criterion will output a NOT AVAILABLE statement just when there is a persistent string of missing echoes.

III. Missing Echoes over a Single Ping

Before examining the compliance of cloud services with the committed availability (i.e., over an observation window), we analyse the behaviour of the cloud over a single ping.

The actual outcome of the testing process is impacted by both network and cloud failures, so that an outage may be declared even when the cloud is perfectly running, thus leading to a false outage declaration. In this section, we examine the

TABLE I
OUTCOMES OF CRITERIA FOR AVAILABILITY STATEMENTS

Ping outcome		Statement		
Replies	Missing echoes	Majority	Un. positive	Un. negative
0	5	NOT AVAIL.	NOT AVAIL.	NOT AVAIL.
1	4	NOT AVAIL.	NOT AVAIL.	AVAIL.
2	3	NOT AVAIL.	NOT AVAIL.	AVAIL.
3	2	AVAIL.	NOT AVAIL.	AVAIL.
4	1	AVAIL.	NOT AVAIL.	AVAIL.
5	0	AVAIL.	AVAIL.	AVAIL.

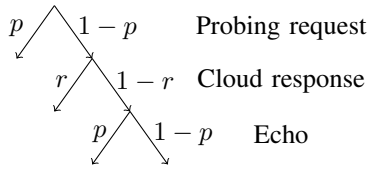


Fig. 4. Sequence of events and pertaining probabilities

testing process in the general case when the cloud may be available, but network failures are also present, and in the two alternative cases when the cloud is either perfectly working (and responding to pings) or not working.

If the cloud is available, we expect to receive a positive echo response for each request, but probing packets routinely get lost due to network failures. If p is the packet loss probability on the testing-station to/from cloud path (we assume that it is the same in either way, and the failures on the two trips are uncorrelated due to time spacing), the resulting sequence for a single probing instance is shown in Fig. 4. There we see how the various path sections contribute to the outcome of the testing process in a single ping, when there is the possibility that the cloud is not working.

If the true cloud outage probability is r, the probability of missing an echo (on a single probing instance) is equal to the sum of the probabilities of the three left branches in the tree of Fig. 4:

$$\begin{aligned} P_{\text{me}} &= p + (1-p)r + (1-p)(1-r)p \\ &= p(2-p) + r(1-p)^2 \simeq 2p + r, \end{aligned} \tag{4}$$

where we see clearly the contribution due to network failures (first term of the sum) and that due to the cloud (second term). In Fig. 5 (showing the true, rather than approximate, P_{me}) we see that the probability of declaring an outage is a linear function of r and biased approximately by a $2p$ term.

The biasing factor P_{me}/r may indeed be very large, as shown in Fig. 6, especially when $p > r$.

This general case may be simplified if we look at the two cases where the cloud is either working or not working.

If we focus on the former case, the response tree reduces to that shown in Fig. 7: two leaves of the binary tree give rise to a negative outcome, and just one (both trips occurring with no packet loss) is reported as successful.

Since the cloud is available, what is reported as a failure is actually a false outage. If we mark by a flag variable X the status of the cloud ($X = 1$ if the cloud is working and 0 otherwise), and by another flag variable Y the outcome of the ping test ($Y = 1$ if we get an echo and 0 otherwise), the

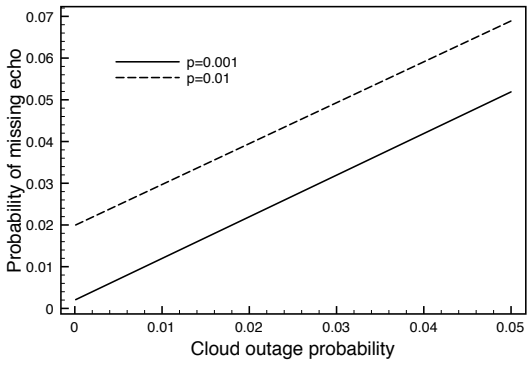


Fig. 5. Probability of missing echo

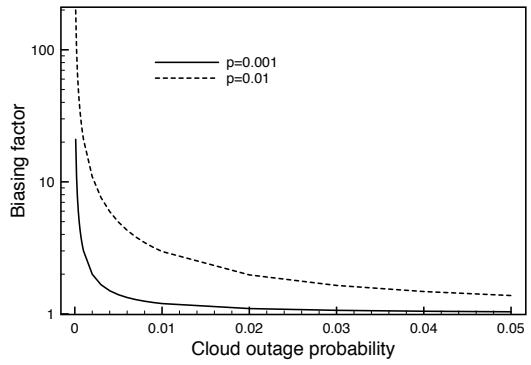


Fig. 6. Biasing factor

probability of a missing echo conditional to the cloud working in a single probing instance is therefore:

$$P_{\text{mecw}} = P[Y = 0|X = 1] = p + (1-p)p = p(2-p) \simeq 2p. \tag{5}$$

In the case that the cloud is not working, of course we will never receive an echo, though the network may be operating correctly.

IV. FALSE OUTAGES OVER A PROBING BURST

If we move from a single ping to a sequence of pings, we have several alternative criteria to declare an outage (a false outage), among which the most relevant have been described in Section II:

- Majority voting;
- Unanimous Positive voting;
- Unanimous Negative voting.

We now evaluate the probability of declaring a false outage under the three criteria when the cloud is perfectly working.

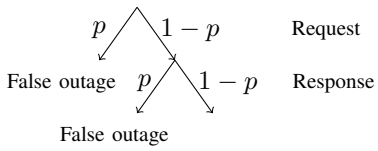


Fig. 7. Sequence of events under no cloud failure

TABLE II
FALSE OUTAGE PROBABILITY OVER A PROBING BURST

Criterion	False outage probability
Majority voting	$\sum_{i=k_{\min}}^{k} \binom{i}{k} P_{\text{mecw}}^{i}(1-P_{\text{mecw}})^{k-i}$
Unanimous Positive voting	$1-(1-P_{\text{mecw}})^{k}$
Unanimous Negative voting	P_{mecw}^{k}

According to Majority Voting, we declare a cloud outage after a sequence of k echo requests when we have at least $k_{\min} = \lceil \frac{k+1}{2} \rceil$ negative responses (no echoes). We assume that the outcomes of successive probing instances in the case of networking failures are uncorrelated. The number of missing echoes in a burst of k requests follows therefore a binomial distribution with parameters p and k. The false outage probability with k probing instances is therefore:

$$P_{\text{fo}}(k) = \sum_{i=k_{\min}}^{k} \binom{i}{k} P_{\text{mecw}}^{i}(1-P_{\text{mecw}})^{k-i} \tag{6}$$

Under the second criterion (Unanimous Positive voting), we must instead receive all echoes in a sequence of k requests to declare the cloud available, or, alternatively, we declare the cloud down in all but one case (all echoes present). Therefore the false outage probability is:

$$P_{\text{fo}}(k) = 1-(1-P_{\text{mecw}})^{k} \tag{7}$$

Finally, the Unanimous Negative voting criterion requires instead that no echoes are received to declare an outage, so that the probability of an outage declaration over k pings is:

$$P_{\text{fo}}(k) = P_{\text{mecw}}^{k} \tag{8}$$

The three cases are summed up in Table II.

The aim of the close repetition of probing instances is anyway to knock down the probability of false outages. In Fig. 8, we see that, for the choice $k = 9$ adopted in [12], the repetition mechanism is highly effective: even when the packet loss probability is quite high ($p = 0.05$), the probability of false outage is as low as $8 \cdot 10^{-10}$ when the Unanimous Negative voting criterion is chosen and $8 \cdot 10^{-4}$ with Majority Voting. However, the Unanimous Positive voting is quite more severe in declaring outages, leading to a high false outage probability (0.6 when the packet loss probability is 0.05). As expected, the Unanimous Negative voting criterion is much more effective than Majority Voting in ruling out false outages, while the Unanimous Positive voting criterion is not at all.

The number of pings in the elementary testing sequence has of course a significant impact. In Fig. 9, plotted for the same packet loss probability $p = 0.01$, we see the exponential fall of the probability of false outages under the Unanimous Negative voting criterion; Majority Voting exhibits a softer descent, whose staircase-like appearance is an artifact due to the majority rule (e.g., when passing from 4 to 5 pings the useful cases are respectively 3 or 4 out of 4, but 3, 4, or 5 out of 5). Instead, the Unanimous Positive voting criterion leads to a false outage probability increasing with the number of pings. This rule proves therefore ineffective in reducing the number of false outages.

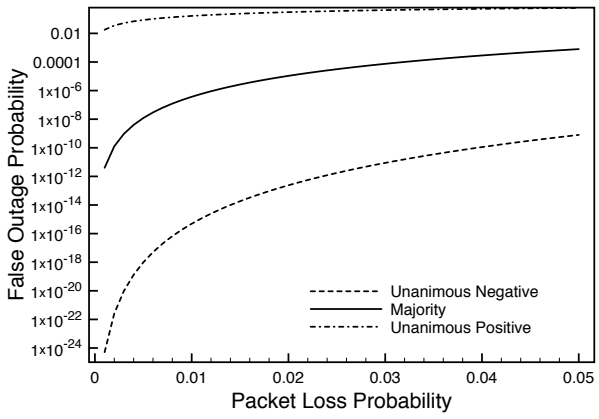


Fig. 8. Probability of false outage (k=9)

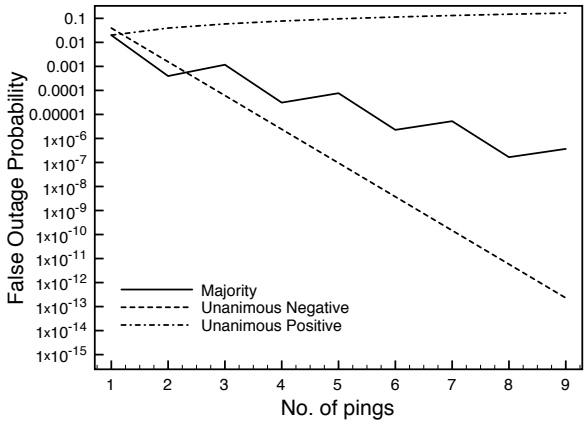


Fig. 9. Impact of the number of retries on false outage probability (p=0.01)

V. AVAILABILITY ESTIMATION OVER A CONTRACT PERIOD

In Sections III and IV we have examined the impact of networking failures on the observed outage probability over two different timescales: a single probing instance and a probing burst. However, the presence of outages is typically assessed to check compliance with Service Level Agreements (SLA). In that case, the check is conducted by comparison with committed availability goals within a (relatively long) observation window . In this section, we examine the availability estimate resulting from the previously described ICMP-based testing approach when an adequately long observation window is considered.

We adopt the testing sequence depicted in Fig. 3. We perform that testing sequence continuously and collect statistics over successive periods of length C, so that C is the observation window prescribed in the SLA. This window must be significantly larger than the testing period T so as to have a large number of testing sequences to perform a statistical estimation of availability. Over any testing period, after sending a burst of k pings, a decision is taken as to the presence of an outage through one of the three criteria described in Section IV. The cloud status resulting from this decision is maintained till the next testing period. If the number

TABLE III
OUTAGE DURATION STATISTICS [MIN]

Company	Average	Standard deviation	CV
Google	506.64	872.58	1.72
Amazon	473.56	1093.18	2.31
Rackspace	607.03	1210.30	1.99
Salesforce	95.2	84.35	0.89
Windows Azure	224.3	165.78	0.74

TABLE IV
ESTIMATED PARAMETERS OF THE GENERALIZED PARETO DISTRIBUTION

Company	scale parameter β	shape parameter ξ
Google	405.29	0.39
Amazon	276.43	-0.12
Rackspace	381.19	0.3
Salesforce	192.47	-0.64
Windows Azure	312.32	-0.35

of testing periods for which an outage has been declared is N_{out}, the availability is estimated as:

$$\hat{A} = 1 - \frac{N_{\text{out}}}{\lfloor C/T \rfloor}, \tag{9}$$

the quantity in the denominator representing the number of testing periods contained in the observation window.

In order to assess the capability of this ICMP-based approach to correctly estimate the availability, we perform a MonteCarlo simulation, where the observed availability is averaged over 1000 simulation instances.

The model of cloud outages is based on the findings of the empirical analysis reported in [15]. The statistics collected over several prominent cloud storage providers are reported in Table III. For each provider a best-fit search was conducted to model the outage durations. It turned out that the outage duration (represented here by the random variable D) is best modelled by a Generalized Pareto distribution, whose cumulative distribution function is [22]:

$$\mathbb{P}[D < x] = G_{\xi,\beta}(x) = \begin{cases} 1 - (1 + \xi x/\beta)^{1/\xi} & \text{if } \xi \neq 0 \\ 1 - e^{-x/\beta} & \text{if } \xi = 0 \end{cases}, \tag{10}$$

where β is the scale parameter and ξ is the shape parameter. The average duration is related to the scale and shape parameters by the expression

$$\overline{D} = \frac{\beta}{1 - \xi}. \tag{11}$$

The optimal values for β and ξ found during that analysis are shown in Table IV.

Here, in order to account for the variety of performances shown in Table IV, we consider a fixed shape parameter $\xi = 0.39$ (the value pertaining to Google) and a scale parameter dictated by the average outage duration $\overline{D}$ through the expression obtained by inverting Equation (11):

$$\beta = \overline{D}(1 - \xi). \tag{12}$$

TABLE V
REFERENCE CASE

Parameter	Value
Observation window C	30 days
Testing Period T	10 minutes
Average Outage Duration $\overline{D}$	500 minutes
No. of pings k	9

In the simulation procedure the durations were generated through the inverse method [23].

The occurrence of outages was instead simulated using a Poisson process with rate λ dictated by the true availability and the average outage duration, following the approach in [24]. By resorting to Wald's identities (see, e.g., Section 34.14.2.11 of [25] or Section 1.7.3 of [26]), we can write the availability as evaluated over the observation window C as:

$$A = 1 - \frac{\mathbb{E}[\sum_{i=1}^{N} D_i]}{C} = 1 - \frac{\overline{N} \cdot \overline{D}}{C} = 1 - \frac{\lambda C \overline{D}}{C} = 1 - \lambda \overline{D}, \tag{13}$$

where N is the number of outages occurring within the period C, and D_i is the duration of the i-th outage. The use of Wald's identities is valid since there is only a weak correlation among the number of summands in the sum in Equation (13) and each of the summands. In fact, the duration of an outage is independent of the number of outages, while the number of outages has a very weak correlation with outage durations, as long as we consider cloud services with high availability. Equation (13) can be easily inverted to find the rate of the Poisson process:

$$\lambda = \frac{1 - A}{\overline{D}}. \tag{14}$$

In order to assess the estimation capabilities of the three decision criteria described in Section IV, we have considered a range of values for the parameters involved in the testing method:

- Observation window length C;
- Testing period length T;
- Number k of pings in each probing burst.

As to the observation window C, we have considered values from 1 to 12 months. A testing period of 10 minutes was adopted in [12], which we mostly maintained, though we have experimented with values from 5 to 15 minutes. As to the number of pings, again in [12] a sequence made of 9 pings was recommended, and we sticked to that choice, though we also considered values as low as 5. However, unless stated otherwise, here we report the results using the reference case described in Table V since we found negligible differences for parameter values outside the reference case.

Finally, the impact of networking failures was accounted for by considering a packet loss probability ranging from 10^{-4} to 10^{-2}.

The range of availability values for which we tested the measurement scheme was [0.95,0.999], which is consistent with what has been reported in several attempts to provide third-party measurements of availability (see, e.g., [15]).

TABLE VI
IMPACT OF THE OBSERVATION WINDOW LENGTH

Observation window [days]	Availability Estimate	
	Majority Voting	Unanimous Positive voting
30	0.9898	0.9981
60	0.9885	0.9982
90	0.9900	0.9982
180	0.9902	0.9982
360	0.9899	0.9982

TABLE VII
IMPACT OF THE TESTING PERIOD

Testing Period [minutes]	Availability Estimate	
	Majority voting	Unanimous Positive voting
5	0.9898	0.9981
10	0.9885	0.9981
15	0.9900	0.9982

We now examine the impact of each of the testing method parameters on the availability estimate by adopting either the Majority Voting criterion or the Unanimous Positive voting one. We rule out the Unanimous Negative voting criterion since in all the experiments it always produced an availability estimate equal to 1, i.e., it never produced an outage statement.

We start with the length of the observation window, for which we observe that it has a negligible influence on the accuracy of the estimation (the accuracy was not tested for lengths shorter than a month). We report in Table VI the results for the reference case (the true availability was set at 0.99): the range of estimates is always below 0.07% of the central value for Majority Voting and 0.01% for Unanimous Positive voting. We note that Majority Voting provides a very good estimate of the true value, while the Unanimous Positive voting criterion always overestimates the actual availability, turning the true 2-nine availability into a nearly 3-nine one.

The impact of the testing period can likewise be considered as negligible, as shown in Table VII, which reports some values obtained for the reference case (where the true availability is 0.99). A similar situation occurred for parameter combinations different from the reference case. Again, we notice the very good estimate delivered by Majority voting, and the overestimate due to Unanimous Positive voting.

This can be considered as valid as long as the testing period does not become comparable with the duration of an outage. If we mark the occurrence of the measurement timepoint preceding the outage as time 0, so that the next measurement takes place at the time T (e.g., 10 minutes as in the reference case), the outage will take place at a random time O such that $0 \leq O \leq T$. If we consider O to be uniformly distributed, the failure will not be detected if the recovery from the outage is achieved before the next measurement interval. If the outage duration is L, that condition can be expressed as $O + L < T$. The probability that the outage goes undetected is then

$$P_{\text{nodet}} = \mathbb{P}[O + L < T] = \mathbb{P}\left[\frac{O}{T} < 1 - \frac{L}{T}\right] = \begin{cases} 0 & \text{if } T \leq L \\ 1 - \frac{L}{T} & \text{if } T > L \end{cases} \quad (15)$$

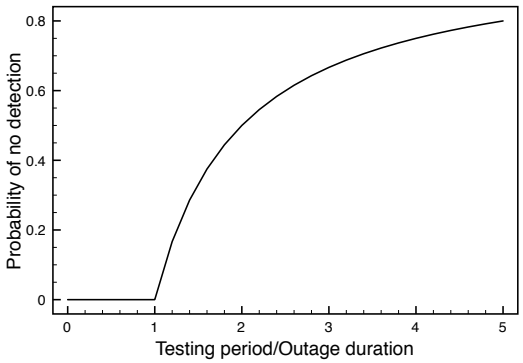


Fig. 10. Probability of an outage going undetected

TABLE VIII
IMPACT OF THE TESTING SEQUENCE LENGTH

No. of pings	Availability Estimate	
	Majority Voting	Unanimous Positive voting
5	0.9893	0.9990
6	0.9902	0.9988
7	0.9905	0.9986
8	0.9899	0.9984
9	0.9898	0.9981

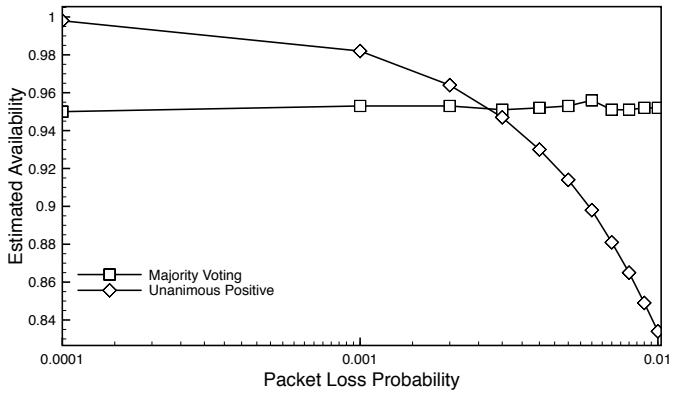
The resulting no-detection probability is shown in Fig. 10.

In that case, it could become difficult to compute the extent of SLA violations and the amount of possible compensations or insurance claims [27][28][29]. In fact, of the three measures (Number of failures; Number of long outages; Cumulative outage duration.) envisaged to be used in an insurance policy for network failures in [24] (but applicable straightforwardly to the case of clouds), just one is considered in [12]. The cumulative outage duration is equal to the overall unavailability, but the number of failures is heavily distorted since short-lived outages may go undetected, and the number of long outages may be underestimated as well, unless the threshold is longer than the measurement interval.

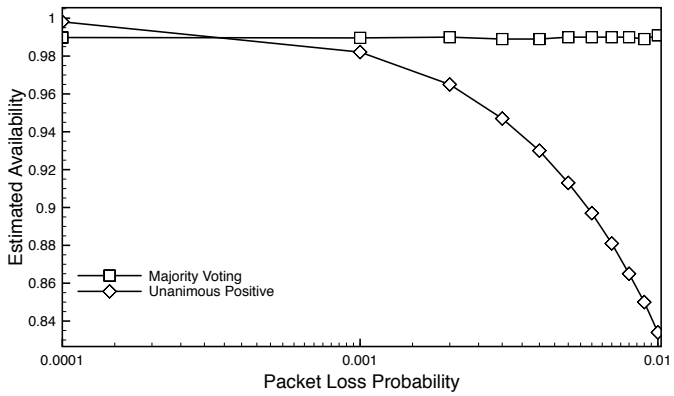
If we now turn to the length of testing sequence, i.e., the number of pings in a probing burst, again we see in Table VIII (which refers to the reference case, with $A = 0.99$, but similar results are obtained for other cases as well) that the impact of the actual number of pings is very small, though for the Unanimous Positive voting criterion the estimate can be seen to decrease as the number of pings grows, providing a better estimate. The choice of $k = 9$ seems therefore the best one in the range examined.

After examining the set of choices for the testing scheme parameters, and having found out that the accuracy is not significantly affected within the range of values considered (with the single exception of the number of pings in a probing burst, for which the highest value is to be preferred), we can now see the impact of networking failures, which is the major source of concern.

In Fig.11, plotted for two values of the true availability ($A = 0.95, 0.99$) and the reference case, we see that the outcome of the Majority Voting criterion is negligibly im-



(a) True Availability = 0.95



(b) True Availability = 0.99

Fig. 11. Availability Estimate

pacted, while the availability estimate is significantly altered under the Unanimous Positive voting criterion. As expected, the situation turns critical as the packet loss probability grows. The turning point can be located around $p = 10^{-3}$, where the estimate starts decreasing, turning from an overestimate into an underestimate as more and more false outages enter the picture. When the packet loss probability is as bad as 10^{-2}, the availability estimate would be so bad as to consider the cloud very unreliable though it actually keeps providing the usual good performance.

The analyses conducted so far, over a wide set of experiments than those reported here, show therefore that significant differences have emerged among the decision criteria we may adopt to declare an outage at each testing period. Precisely, the Majority Voting criterion has always provided a correct estimate, while the Unanimous Positive voting criterion typically errs on the plus side (overestimating the availability) when the packet loss probability is small enough, but instead grossly underestimates the availability when the packet loss probability exceeds 10^{-3}.

VI. Conclusion

We have evaluated the accuracy of a cloud availability estimation method based on the periodic repetition of sequences of probing packets (the pings made available in the ICMP protocol) by MonteCarlo simulation. Three different criteria (Majority voting, Unanimous Positive voting, and Unanimous Negative voting) have been compared to output an availability statement. Majority Voting provides an accurate statement over a wide range of testing parameters and context scenarios, even when the packet loss probability, a major source of false outages, is rather high. Instead, the Unanimous Positive voting criterion, outputting an availability statement just after all the pings in a sequence have received an echo, can lead to gross underestimation when the packet loss probability exceeds 10^{-3}. The Unanimous Negative voting criterion, always outputting an availability statement unless no echoes are received in a probing sequence, is completely unreliable, providing a statement of 100% availability in all the cases examined. The Majority Voting is therefore the criterion of choice in the ICMP-based method to estimate the availability of a cloud.

References

[1] J. Montes, A. Sánchez, B. Memishi, M. S. Pérez, and G. Antoniu, "Gmone: A complete approach to cloud monitoring," *Future Generation Computer Systems*, vol. 29, no. 8, pp. 2026–2040, 2013.

[2] Z. Li, L. O'Brien, H. Zhang, and R. Cai, "On a catalogue of metrics for evaluating commercial cloud services," in *Grid Computing (GRID), 2012 ACM/IEEE 13th International Conference on*, Sept 2012, pp. 164–173.

[3] R. N. Calheiros, R. Ranjan, A. Beloglazov, C. A. F. De Rose, and R. Buyya, "Cloudsim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," *Software: Practice and Experience*, vol. 41, no. 1, pp. 23–50, 2011.

[4] A. Cuomo, G. Di Modica, S. Distefano, A. Puliafito, M. Rak, O. Tomarchio, S. Venticinque, and U. Villano, "An sla-based broker for cloud infrastructures," *Journal of Grid Computing*, vol. 11, no. 1, pp. 1–25, 2013.

[5] V. C. Emeakaroha, M. A. Netto, R. N. Calheiros, I. Brandic, R. Buyya, and C. A. D. Rose, "Towards autonomic detection of {SLA} violations in cloud infrastructures," *Future Generation Computer Systems*, vol. 28, no. 7, pp. 1017 – 1029, 2012.

[6] E. Casalicchio and L. Silvestri, "Mechanisms for SLA provisioning in cloud-based service providers," *Computer Networks*, vol. 57, no. 3, pp. 795–810, 2013.

[7] Y.-S. Dai, B. Yang, J. Dongarra, and G. Zhang, "Cloud service reliability: Modeling and analysis," in *15th IEEE Pacific Rim International Symposium on Dependable Computing*, 2009.

[8] K. V. Vishwanath and N. Nagappan, "Characterizing cloud computing hardware reliability," in *Proceedings of the 1st ACM symposium on Cloud computing SoCC*. ACM, 2010, pp. 193–204.

[9] A. Li, X. Yang, S. Kandula, and M. Zhang, "Cloudcmp: comparing public cloud providers," in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*, 2010, pp. 1–14.

[10] B. Calder, J. Wang, A. Ogus, N. Nilakantan, A. Skjolsvold, S. McKelvie, Y. Xu, S. Srivastav, J. Wu, H. Simitci *et al.*, "Windows azure storage: a highly available cloud storage service with strong consistency," in *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*. ACM, 2011, pp. 143–157.

[11] D. Ford, F. Labelle, F. I. Popovici, M. Stokely, V.-A. Truong, L. Barroso, C. Grimes, and S. Quinlan, "Availability in globally distributed storage systems," in *9th USENIX Symposium on Operating Systems Design and Implementation, OSDI 2010*, Vancouver, BC, Canada, October 4-6, 2010, pp. 61–74.

[12] Z. Hu, L. Zhu, C. Ardi, E. Katz-Bassett, H. Madhyastha, J. Heidemann, and M. Yu, "The need for end-to-end evaluation of cloud availability," in *Passive and Active Measurement*, ser. Lecture Notes in Computer Science, M. Faloutsos and A. Kuzmanovic, Eds. Springer International Publishing, 2014, vol. 8362, pp. 119–130.

[13] M. Naldi, "A note on "the need for end-to-end evaluation of cloud availability"," *arXiv CoRR Preprint Series*, vol. abs/1408.0510, 2014.

[14] C. Cérin, C. Coti, P. Delort, F. Diaz, M. Gagnaire, Q. Gaumer, N. Guillaume, J. L. Lous, S. Lubiarz, J.-L. Raffaelli, K. Shiozaki, H. Schauer, J.-P. Smets, L. Séguin, and A. Ville, "Downtime statistics of current cloud solutions," Available at http://iwgcr.org/wp-content/uploads/2013/06/IWGCR-Paris.Ranking-003.2-en.pdf, June 2013.

[15] M. Naldi, "The availability of cloud-based services: Is it living up to its promise?" in *9th International Conference on the Design of Reliable Communication Networks, DRCN 2013, Budapest, Hungary*, March 4-7, 2013, pp. 282–289.

[16] ——, "Accuracy of Third-Party Cloud Availability Estimation through ICMP," in *39th International Conference on Telecommunications and Signal Processing (TSP)*. Vienna: IEEE, 2016.

[17] G. Hogben and A. Pannetrat, "Mutant apples: a critical examination of cloud sla availability definitions," in *Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on*, vol. 1. IEEE, 2013, pp. 379–386.

[18] J. Postel, "Internet control message protocol," ISI Network Working Group Request for Comments 792, 1981.

[19] D. Ford, F. Labelle, F. I. Popovici, M. Stokely, V.-A. Truong, L. Barroso, C. Grimes, and S. Quinlan, "Availability in globally distributed storage systems." in *OSDI*, 2010, pp. 61–74.

[20] D. D. Long, J. L. Carroll, and C. Park, "A study of the reliability of internet sites," in *Reliable Distributed Systems, 1991. Proceedings., Tenth Symposium on*. IEEE, 1991, pp. 177–186.

[21] G. Huston, "Measuring ip network performance," *The Internet Protocol Journal*, vol. 6, no. 1, pp. 2–19, 2003.

[22] A. J. McNeil and T. Saladin, "The peaks over thresholds method for estimating high quantiles of loss distributions," in *Proceedings of 28th International ASTIN Colloquium*, 1997, pp. 23–43.

[23] I. Mierlus-Mazilu *et al.*, "On generalized pareto distributions," *Romanian Journal of Economic Forecasting*, p. 107, 2010.

[24] L. Mastroeni and M. Naldi, "Network protection through insurance: Premium computation for the on-off service model," in *8th International Workshop on the Design of Reliable Communication Networks DRCN, Krakow, Poland*, 10-12 October 2011, pp. 46–53.

[25] A. D. Poularikas, *The Handbook of Formulas and Tables for Signal Processing*. CRC Press, 1999, ch. Probability and Stochastic Processes.

[26] F. Beichelt, *Stochastic Processes in Science, Engineering and Finance*. Chapman & Hall/CRC, 2006.

[27] M. Naldi and L. Mastroeni, "Violation of service availability targets in service level agreements," in *Federated Conference on Computer Science and Information Systems - FedCSIS 2011, Szczecin, Poland*, 18-21 September 2011, pp. 537–540.

[28] L. Mastroeni and M. Naldi, "Compensation policies and risk in service level agreements: A value-at-risk approach under the on-off service model," in *Economics of Converged, Internet-Based Networks - 7th International Workshop on Internet Charging and QoS Technologies, ICQT 2011, Paris, France*, ser. Lecture Notes in Computer Science, vol. 6995. Springer, October 24, 2011, pp. 2–13.

[29] P. Cholda, E. L. Følstad, B. E. Helvik, P. Kuusela, M. Naldi, and I. Norros, "Towards risk-aware communications networking," *Rel. Eng. & Sys. Safety*, vol. 109, pp. 160–174, 2013.

Analyzing Influence of the Transmission Medium on Timing Signals Transmitted by Hybrid Optical Transport Technologies

Rastislav Róka and Veronika Dolinayová

***Abstract*— The contribution deals with synchronization aspects in SDH and Synchronous Ethernet timing networks utilizing optical transmission medium. First, it explains a hierarchical configuration of timing network elements, characterizes transmission features of the optical fiber, particularly its main negative influences influencing transmitted information signals. The main part is dedicated to the evaluation program created for analyzing influences of the optical transmission path on timing signals transmitted by SDH and SyncE transport technologies. At last, resultant values from the introduced evaluation program are presented and evaluated.**

***Keywords*— optical transmission medium, SDH and Synchronous Ethernet Technologies, timing networks, transmission parameters.**

I. Introduction

For developing future services and applications [1], [2], solving of synchronizations for digital signals transmitting in telecommunication networks must be globally applicable and beneficial. Therefore, synchronization is one from key aspects at the signal transmission through metallic, optical or other transmission media by various different technologies [3], [4]. From the synchronization viewpoint, digital transmission networks can be divided into two groups – synchronous and asynchronous. In this contribution, we focus on timing signals transmitted by SDH (Synchronous Digital Hierarchy) and SyncE (Synchronous Ethernet) technologies utilizing the optical transmission medium.

For the signal transmission in SDH and Synchronous Ethernet networks, a dominating transmission medium is the optical fiber. It is a fact that various negative environmental effects influence any information or timing signals transmitted through the optical transmission medium. To the most important belong an attenuation occasioning the optical impulse's amplitude decreasing and a dispersion occasioning the optical impulse's time expansion. From a viewpoint of digital transmission technologies, these effects become expressively evident by changing of transmission parameters. Therefore, a maximum transmission rate in the optical medium is finite and a signal is transmitted to the definite transmission distance depending on the optical source, parameters of the optical fiber and the optical receiver at the optical transmission path's end. In this contribution, the aim is focusing on the optical transmission medium and its impact on transmission parameters of timing signals utilized by SDH and Synchronous Ethernet technologies. The created evaluation program can be utilized for evaluation of exploited optical transmission paths transmitting digital signals of future services and applications.

Manuscript received August 15, 2016, revised January 19, 2017.

This article was created with the support of the Ministry of Education, Science, Research and Sport of the Slovak Republic within the KEGA agency project - 007STU-4/2016 "Progressive educational methods in the field of telecommunications multiservice networks" and VEGA agency project - 1/0462/17 "Modeling of qualitative parameters in IMS networks".

Rastislav Róka is with Institute of MICT, FEI STU, Bratislava, Slovakia (corresponding author, phone: 421-2-68279608; e-mail: rastislav.roka@stuba.sk).

Veronika Dolinayová was with Institute of MICT, FEI STU, Bratislava, Slovakia (e-mail: veronika.dolinayova@gmail.com).

doi: 10.11601/ijates.v6i1.186

II. SDH and Synchronous Ethernet timing networks

A. SDH timing network

A timing architecture in the SDH digital transmission network is hierarchical, thus every network node has its specific frequency, respectively timing accuracy. This architecture is splitted into 4 layers with strictly defined timing accuracies [5]. Individual SDH timing network elements include build-in frequency generators with the certain accuracy that is not absolutely identical for all elements. Deviations from the nominal synchronization frequency transmitted from node to node are summed and, in consequence, the crash of synchronization can come into the existence at the optical transmission path's end. From this reason, a common primary source of the timing signal is established with the highest Stratum 1 accuracy in the hierarchical structure [5].

A structure of timing elements in the SDH network is hierarchical, defined as the master-slave structure. A basic arrangement is the synchronizing chain, where at the highest level is presented by the PRC (Primary Reference Clock) clock. The second level below is formed by the SSU (Synchronization Supply Unit) clock. The SEC (Synchronous Equipment Clock) clock on the lowest level with the minimum accuracy demand is located in individual SDH timing network elements. According to ITU-T recommendations, the maximum number of elements coupled in the synchronizing chain is defined as

follows: a maximum of 20 SEC elements located between 2 SSU elements, a maximum of 10 SSU elements and 59 SEC elements in the common chain [5], [6]. The ITU-T recommendation [7] describes the functional architecture of transport networks including network synchronization principles for networks that are based on the SDH.

B. Synchronous Ethernet timing network

The Synchronous Ethernet technology is defined in the ITU-T Q13/15 recommendation, where a distribution of timing signals in the SyncE network is specified. The reference timing signal from the PRC clock is distributed in the Synchronous Ethernet network by similar mechanisms as in the SDH network. Above all, a timing signal is separated from information, managing and controlling signals and then is transmitted through the physical layer [8].

The IETF (Internet Engineering Task Force) organization specified the CES (Circuit Emulation Service) element for interconnecting SDH and Synchronous Ethernet timing networks. For correct interoperability and cooperation between these two networks, the CES element is referred to be as the slave and must have the same synchronization features as the SEC one. A maximum number of CES elements in the synchronizing chain is defined 20 [9]. The ITU-T recommendation [7] also includes the application of various mappings.

III. Transmission Features of the Optical Transmission Path

A. Attenuation in the optical transmission medium

The attenuation, alternatively the loss, is depending on the wavelength and is composed from scattering, absorption and bending parts. The total attenuation can be calculated using the formula [5]:

$$a = \alpha \cdot L, \tag{1}$$

where a is the attenuation in [dB], α is the specific attenuation in [dB/km] and L represents the optical fiber length in [km]. This attenuation simultaneously corresponds to a difference between the transmitter power and the receiver sensitivity and, therefore, can be used for determination of the maximum transmission distance.

B. Dispersion in the optical transmission medium

The dispersion is composed from three main parts - modal, chromatic and polarization mode. The modal dispersion is due to various track lengths of particular modes and is present in multi-mode optical fibers. In single-mode fibers, the chromatic dispersion depending on the spectral bandwidth of optical sources becomes evident. In these fibers, the polarization mode dispersion is also originating and, therefore, a resultant value is given from contributions of both CD and PMD components [10]. Then, a final time expansion of the transmitted optical impulse is determined. For successful and reliable separation of particular optical impulses, a maximum transmission rate of the digital signal is limited by a following equation:

$$R_b = \frac{1}{T_b}, \tag{2}$$

where R_b is the transmission bit rate in [bit/s] and T_b is the time duration of one information bit in [s]. For correct detecting of the information optical impulse, a maximum of its time expansion is theoretically limited to a half of the time duration of one information bit. For more real approximation, a possible impulse time expansion is set to the $1/10 \cdot T_b$ value in the program.

C. Parameters of used components

A optical transmission path utilizing the optical transmission medium is composed from following components:

- a source of the optical radiation,
- an optical fiber,
- a detector of the optical radiation.

Concrete values related to the source power, the specific attenuation and dispersion of the optical fiber and the receiver sensitivity used in the created evaluation program can be found in [11]–[16].

IV. The Evaluation Program

The core of this contribution is an evaluation program for analyzing influences of the optical transmission medium on timing signals transmitted by hybrid transport technologies through evaluating transmission parameters. It is created by using the MatLab programming environment.

In timing networks, we can distinguish 4 basic types of the synchronization clock (Type I – IV) that are determined by their accuracy (in a time and/or frequency domain). These four synchronization clocks are organized in the hierarchical timing structure where the strongest requirements are defined for the highest level related to the PRC. The Primary Reference Clock represents the Type I clock. For this reason, it is satisfactory to focus our attention only on the Type I level. Other clocks located on lower levels are constrained with less rigorous demands. The Appendix III in [7] contains concrete guidelines for synchronization network engineering where all aspects related to the arrangement of synchronization clocks are explained by detail. For timing signals transmitted in the optical transmission medium, it is important to specify a concrete carrier wavelength of the optical radiation. For selecting adequate sources of the optical radiation, these specific source wavelengths together with their spectral bandwidth (deviations) are important.

For the Type I clock, a defined maximum deviation for the timing signal is 1,5 nm modulated at the source wavelength. Typical utilized source of the optical radiation in practical transmission systems has a broader defined minimum spectral bandwidth [11]. Because a bandwidth of the modulated timing signal is included in this minimum spectral bandwidth, the Type I clock timing signal is not necessary to adapt for transmitting through the optical medium. Hereby, it is satisfactory to consider only mentioned source spectral bandwidth in the evaluation

program.

A. *Graphical interface*

After running the program, the opening screen is displayed (Fig. 1).

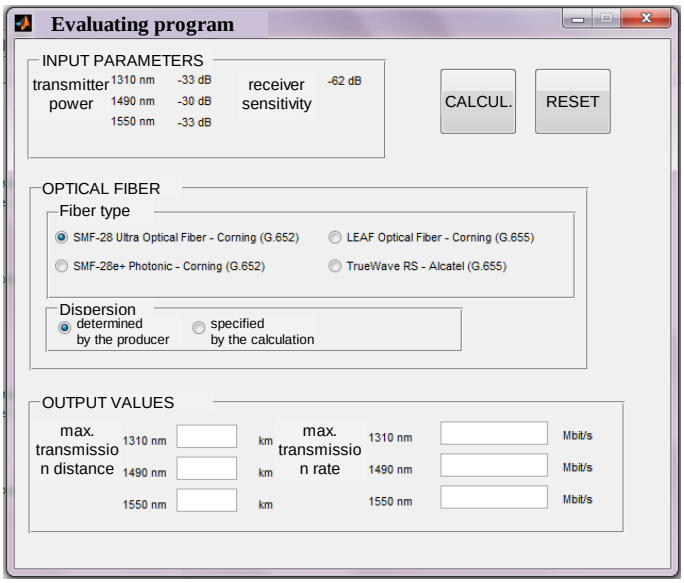


Fig. 1: The graphical interface of the evaluation program

In the first evaluation step, parameters for the source and the detector of the optical radiation are presented. Consequently, using input values of the transmitter power P_{tran} in [dB] and the receiver sensitivity S_{rec} in [dB] together with the specific attenuation value α_{OF} in [dB/km] for the selected fiber type, a calculation can be executed for defined wavelengths. A maximum transmission distance L of the optical path transmission can be calculated using a following formula resulting from the formula (1):

$$L = \frac{1}{\alpha_{OF}} \left(10 \cdot \log \frac{P_{trans}}{S_{rec}} \right), \tag{3}$$

In the evaluation program, considered optical fibers are presented. In the part "Fiber type", 4 considered kinds of optical fibers are included - two are based on the ITU-T G.652 standard [17] and two on the ITU-T G.655 standard [18]. Parameters of these fiber types are used in both evaluation steps by appropriate way. As a default choice, the Corning SMF-28 Ultra optical fiber and values determined by the producer are predetermined.

In the second evaluation step, an approach for dispersion calculating must be selected. There come into consideration two choices - concrete values determined by the producer or values considering the spectral bandwidth of the source. Using obtained values of the chromatic dispersion D_{CH} in [ps/(nm.km)]] for the selected fiber type and the source spectral bandwidth BW_{source} in [nm] together with the calculated maximum transmission distance L, a calculation can be executed for defined wavelengths. A transmission rate R_b of the optical information signal can be calculated using following formulas resulting from the formula (2):

$$\Delta t_{CH} = \frac{D_{CH}}{BW_{source} \cdot L}, \tag{4}$$

$$R_b = \frac{1}{10 \cdot \Delta t_{CH}}, \tag{5}$$

where Δt_{CH} is the impulse time expansion in [ps] due to the chromatic expansion of optical fibers.

Finally, output values of the evaluation are presented. Here, the maximum transmission distance L [km] of the optical radiation together with the maximum transmission rate R_b [Mbit/s] of the information signal are displayed for particular source wavelengths.

B. *Resultant values for the maximum transmission distance and transmission rates*

Resultant values of the maximum transmission distance L and transmission rates $R_{b\,det}$ and $R_{b\,func}$ for Corning SMF-28 Ultra and Corning SMF-28e+ Photonic optical fibers are introduced in Tables I and II. The transmission rate $R_{b\,det}$ is calculated based on values determined by the producer, the transmission rate $R_{b\,func}$ is calculated from functionally dependent values on wavelengths for the specific attenuation and chromatic dispersion.

TABLE I
RESULTANT VALUES FOR THE CORNING SMF-28 ULTRA OPTICAL FIBER

λ [nm]	L [km]	$R_{b\,det}$ [Mbit/s]	$R_{b\,func}$ [Mbit/s]
1310	82,8571	109 858,8	18,3291
1490	160,000	79 056,9	7,4452
1550	145,000	0,9576	0,8900

TABLE II
RESULTANT VALUES FOR THE CORNING SMF-28E+ PHOTONIC OPTICAL FIBER

λ [nm]	L [km]	$R_{b\,det}$ [Mbit/s]	$R_{b\,func}$ [Mbit/s]
1310	82,8571	109 858,8	16,7498
1490	133,333	86 602,5	9,3439
1550	145,000	0,9576	0,9687

The Corning SMF-28 Ultra and Photonic optical fibers correspond to the ITU-T G.652 standard [17]. They present classical single-mode fibers used in telecommunications. The zero value of the chromatic dispersion is located around the 1310 nm wavelength, where the maximum achievable rate $R_{b\,det}$ approximately 100 Gbit/s is resulting. When a spectral bandwidth of the optical source is considering together with a functional dependency on wavelengths for the chromatic dispersion, a theoretical maximum achievable rate $R_{b\,func}$ is decreased to tens of Mbit/s. A value of the chromatic dispersion determined by the producer at the 1550 nm wavelength is approximately the same as a functionally dependent value, therefore maximum achievable transmission rates are roughly equal for both cases.

A specific attenuation of the SMF-28 Ultra optical fiber has the lowest value at the 1490 nm wavelength. It means that the longest transmission distance L can be reached

exactly at this wavelength. For this case, however, a transmission rate is decreased due to the signal transmission over this distance. The lowest value of the specific attenuation for the SMF-28e+ Photonic optical fiber is present at the 1550 nm wavelength; hence a signal travels the longest transmission distance at this wavelength for given fiber.

Resultant values of the maximum transmission distance L and transmission rates $R_{b\,det}$ and $R_{b\,func}$ for Corning LEAF and Alcatel Lucent TrueWave RS optical fibers are introduced in Tables III and IV.

TABLE III
RESULTANT VALUES FOR THE CORNING LEAF OPTICAL FIBER

λ [nm]	L [km]	$R_{b\,det}$ [Mbit/s]	$R_{b\,func}$ [Mbit/s]
1310	85,2941	12,4349	11,0904
1490	145,4545	23,2488	23,0484
1550	138,0952	4,5259	2,9817

TABLE IV
RESULTANT VALUES FOR THE ALCATEL LUCENT TRUEWAVE RS OPTICAL FIBER

λ [nm]	L [km]	$R_{b\,det}$ [Mbit/s]	$R_{b\,func}$ [Mbit/s]
1310	72,5000	3,8314	3,3642
1490	106,6667	69,4444	64,1026
1550	116,0000	3,5920	2,9727

The Corning LEAF and Alcatel Lucent TrueWave RS optical fibers correspond to the ITU-T G.655 standard [18]. They present optical fibers with the shifted zero value of the chromatic dispersion to the 1550 nm wavelength surroundings. For both kinds, the producer determined a functional dependency of the chromatic dispersion on wavelengths. Therefore, values of the maximum theoretical transmission rates are approximately equal in both cases. Both optical fibers reach the maximum transmission rates around the 1490 nm wavelength. The TrueWave RS optical fiber reaches higher transmission rate at this wavelength, however a signal travels shorter transmission distances compared with the LEAF optical fibers. From calculated values, we can consider that the TrueWave RS directional vector forms a bigger angle with the horizontal axis than the LEAF one for about linear functional dependencies on wavelengths for the chromatic dispersion.

In practice, results from the evaluation program can be used in different ways, for instance at a selection of the wavelength for the optical channel with given transmission rates, respectively at a determination of the transmission rate for selected wavelengths. Just as well, a specifying of the source working wavelength for the longest transmission distance on the optical fiber's parameters can be realized based on presented resultant values. Globally, the presented evaluation program with analyzing of specific optical fibers can be utilized for evaluation of exploited optical transmission paths transmitting digital signals. In consequence, applicability and benefits of the optical transmission medium for transmitting timing signals for developed future services and applications and global telecommunication networks can be determined.

V. CONCLUSION

The program for analyzing influences of the optical transmission medium on timing signals transmitted by hybrid transport technologies through evaluating transmission parameters is created and related to a synchronization in SDH and Synchronous Ethernet timing networks.

A timing signal travelling through the optical fiber is influenced by various negative environmental effects. To the most expressive ones belong an attenuation and a dispersion, therefore it is important to know exact values for these parameters and/or exact functional dependencies on wavelengths for given parameters. From this reason, a timing signal is travelling through the optical transmission path with a finite transmission rate on a definite transmission distance. Results from the evaluation program prove that there can be found marked differences based on approaches to the dispersion characteristics for some types of optical fibers. These differences can lead to significant problems at the practical realization of multiple optical channel transmissions in hybrid transport systems using a wavelength division multiplexing technique.

The created evaluation program satisfies essential demands for determination a maximum transmission distance and a maximum transmission rate of timing signals transmitted through the optical transmission path. The program is created in the MatLab programming environment with a simple and comprehensible graphical interface. In a near future, possibilities for selecting of source, optical fibers and detectors can be easily extended. Moreover, other optical components (namely connectors, couplers, welds, …) utilized in conjunction with the optical fiber can be included for analyzing influences of the optical transmission medium on timing signals.

In the next phase, an influence of network nodes included in the optical transmission path will be analyzed. For this intention, two direction of research are considered. First, network nodes realized with electro-optical and opto-electrical conversions will be supposed. Second, network nodes with only optical processing and controlling of timing signals are assumed.

REFERENCES

[1] M. Kellovský, I. Baroňák, M. Kavacký, E. Chromý, "The Optimal Sizing of HSS Database in IMS", *Wireless Personal Communications*, vol. 86, 2016, pp. 1-14, doi:10.1007/s11277-016-3750-6.

[2] J. Sitárová, M. Maár, M. Orgoň, "The Enterprise Telecommunication Network Design and its Implementation Using Technology PLC", *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 4, 2016, pp. 95-104.

[3] S. Klúčik, E. Chromý, I. Baroňák, "Model to increase the number of output sates of a random variable using a histogram based PDF", *Wireless Personal Communications*, vol. 85, 2015, pp. 137-149, doi:10.1007/s11277-015-2731-5.

[4] M. Nízky, M. Orgoň, "Mobile Antenna Inetvu 1800+ Series and Its Implementation in Practice", *International Journal of Wireless and Microwave Technologies*, January 2016, doi:10.5815/ijwmt.

[5] V.K. Stamarions, *Understanding SONET/SDH and ATM Communications Networks for the Next Millennium*. Lucent Technologies, USA, 1999, ISBN 0-7803-4745-5.

[6] J. Ferrant, *SDH Synchronization*. London, United Kingdom, October 2005, available: http://www.scribd.com/doc/57003844/SDH-Synchronization.
[7] *Architecture of transport networks based on the synchronous digital hierarchy (SDH)*, ITU-T Recommendation G.803, 2000.
[8] A. Magree, "Synchronization in Next-Generation Mobile Backhaul Networks", *IEEE Comm. Magazine*, vol. 48, 2010, pp. 110 – 116.
[9] Z. Ghebretensaé, J. Harmatos, K. Gustafsson, "Mobile Broadband Backhaul Network Migration from TDM to Carrier Ethernet", *IEEE Communications Magazine*, vol. 48, 2010, pp. 102 – 109.
[10] J. Čuchran, R. Róka, *Optocommunication Systems and Networks*. STU Publishing House, Bratislava, 2000, ISBN 80-227-2437-8.
[11] ThorLabs. *Coherent Sources-Laser Diodes by Wavelength*. available (20/10/2016): https://www.thorlabs.com/navigation.cfm
[12] *Corning SMF-28 Ultra Optical Fiber*. available (20/10/2016): https://www.corning.com/media/worldwide/coc/documents/Fiber/SMF-28 Ultra.pdf
[13] *Corning SMF-28e+ Photonic Optical Fiber*. available (20/10/2016): http://www.corning.com/media/worldwide/csm/documents/Photonic Fiber_040113_uploaded 12_15_15.pdf
[14] *Corning LEAF Optical Fiber*. available (20/10/2016): http://www.corning.com/media/worldwide/coc/documents/Fiber/PI1107_07-14_English.pdf
[15] *Lucent TrueWave RS – Nonzero-dispersion optical fiber*. available (20/10/2016): http://www.telepp.com/support/broadband_coax/truewave/true_wave.pdf
[16] OSI LaserDiode. *InGaAs APD/PIN Modules*. available (20/10/2016): http://www.laserdiode.com/standard_products.
[17] *Characteristics of a single-mode optical fiber and cable*, ITU-T Recommendation G.652, 2009.
[18] *Characteristics of a non-zero dispersion-shifted single-mode optical fiber and cable*, ITU-T Recommendation G.655, 2009.

Rastislav Róka was born in Šaľa, Slovakia on January 27, 1972. He received his M.Sc. and Ph.D. degrees in Telecommunications from the Slovak University of Technology, Bratislava, in 1995 and 2002. Since 1997, he has been working as a senior lecturer at the Institute of Telecommunications, Faculty of Electrical Engineering and Information Technology, Slovak University of Technology in Bratislava. Since 2009, he is working as an associated professor at this institute.

His research and educational activities are focused on the signal transmission realized in fixed transmission media, optocommunication transmission systems and networks. A main effort is dedicated to effective utilization of the optical fiber's transmission capacity by using various optical signal processing techniques and dynamic bandwidth and wavelength allocation algorithms.

Veronika Dolinayová was born in Žilina, Slovakia on October 10, 1992. She received her M.Sc. degree in Telecommunications from the Slovak University of Technology, Bratislava, in 2016.

A High Speed Architecture for Lifting-based 2-D Cohen-Daubechies-Feauveau (5,3) Discrete Wavelet Transform used in JPEG2000

Mohammad Rafi and Najeed-ud-Din

***Abstract*—For real-time applications, efficient VLSI implementation of DWT is desired. In this paper, DWT architecture based on retiming for pipelining and unfolding is presented. The architecture is based on lifting one-dimensional Cohen-Daubechies-Feauveau (CDF) (5,3) wavelet filter, which is easily extended to 2-D implementation. It consists of low complexity and easily repeatable components. This paper is focused on the critical path minimization and throughput optimization at the same time. The architecture has been implemented on Virtex 6 Xilinx FPGA platform. The implementation results show that the critical path is minimized four to five times, while throughput is doubled, making the overall architecture approximately ten times faster when compared with the conventional lifting-based DWT architecture. Further with parallel implementation, the throughput has doubled without any increase in number of row buffers, implying that the architecture is memory efficient as well. The even and odd rows of the image are scanned in parallel fashion. To perform the 2-D DWT transform of an image of size 15 Megapixels, it takes 16.86 ms, which implies 59 images of that size can be processed in one second. This can be utilized for real-time video processing applications even for high resolution videos.**

I. Introduction

The discrete wavelet transform (DWT) has completely replaced the discrete cosine transformation (DCT) in image coding because it supports progressive image transformation, multi-resolution, ease of compressed image manipulation, region of interest coding, etc. Traditionally, DWT was implemented using convolution. Such an implementation requires both, a large number of computation and a large storage which are undesirable for any high speed or low power application. A new mathematical formulation that replaces the convolution-based wavelet transformation [1]–[4] has been proposed by Sweldens [5], [6], namely lifting-based wavelet transformation. The main feature of the lifting-based discrete wavelet transform scheme is to break up the high-pass and low-pass wavelet filters into a sequence of smaller filters that in turn can be converted into a sequence of upper and lower triangular matrices. The idea behind the lifting scheme is to use data correlation to remove the redundancy. Some of the advantages of this reformulation of the DWT includes "in-place" computation of the DWT, integer-to-integer wavelet transform (IWT), symmetric forward and inverse transform, suitability of parallelism and many more [7]. The lifting scheme decomposes every DWT operation into a sequence of lifting steps. The basic steps involved are splitting, predicting and updating [8]. Further the filters may be classified into 2M consisting of one predict and one update step and 4M consisting of two predict and two update steps.

The state-of-the-art compression technique, JPEG2000, is striving for the development of efficient architecture of wavelet transform. Presently JPEG2000 uses Cohen-Daubechies-Feauveau (5,3) and (9,7) wavelet filters for lossless and lossy compression schemes respectively [9]–[11]. CDF (5,3) wavelet filter is 2M based, while CDF (9,7) is 4M based; 2M consists of one predict and one update stage, while 4M consists of two predict and two update stages. (5,3) indicate that the number of highpass and lowpass filter taps are 5 and 3 respectively. Since (5,3) and (9,7) are used in JPEG2000, lot of work has been done for their efficient implementation. The parameters under consideration are: speed, throughput, computational complexity and memory reduction. A few papers have worked on reduction of critical path as well.

Advantages of lifting-scheme over convolution-based has been presented in [12] for wavelet (9,7). [13] has presented a survey on different VLSI architectures on lifting based DWT. Architectures for reduction of memory accesses and hardware complexity have been proposed in [14]–[17]. Throughput optimization has always had a trade-off with architectural area. Few papers that have proposed architectures for throughput optimization are [16], [17]. Speed can also be increased by reducing the critical path delay of a design. But critical path reduction is always obtained at the cost of increase in latency and number of registers. The papers that have worked on critical path minimization are [18], [19]. The implementation of most of these architectures is based on FPGA using VHDL synthesis, however MATLAB/Simulink/Xilinx System Generator can also be utilized for the same [20], which helps portability and rapid time-to-market of the architecture. Many of the papers have aimed at either multiplier less architecture or shift based multipliers [14]. The other wavelet filters which are frequently considered for optimization are Daubechies-4 (D4), Daubechies-6 (D6), Daubechies-8 (D8), CDF (2,2), (6,10) etc. Universal embedded hardware implementation of a variety of wavelet kernels have been implemented in [8], [21]. The implementation methods are either based on parallel architecture of each kernel or processing element (PE). The parallel

Manuscript received October 7, 2016, revised January 31, 2017

M. Rafi is with the Department of Electronics and Communication Engineering, National Institute of Technology, Srinagar 190 006 India (phone: +91-9622-515357; e-mail: mohdrafi_11phd13@nitsri.net).

Najeeb-ud-Din is with the Department of Electronics and Communication Engineering, National Institute of Technology, Srinagar 190 006 India(e-mail: najeeb@nitsri.net).

method implements multiple wavelet kernels in parallel, which helps in increasing speed at the cost of some extra hardware. While in processing element method, resources are shared between different wavelet kernels, hence lesser resources are needed as compared to parallel implementation.

The proposed work exploits the critical path of the design by using algorithms for retiming for pipelining and unfolding. The throughput of the proposed architecture has increased while as the computation time has reduced when compared with the conventional lifting architecture. The rest of the paper is organized as follows. Section II provides a brief introduction of the CDF (5,3) filter and its implementation. Section III describes the proposed algorithm and architecture. The implementation results are provided in Section IV. Finally, concluding remarks are given in Section V.

II. 2-D CDF (5,3) Discrete Wavelet Transform

A. Mathematical Formulation

The standard lifting scheme has been divided into three stages: Split, predict and update as discussed in [5] and [7].
Split: The original input sequence and the filter coefficients are split into two branches of even and odd components. To make sure that each branch gets only its desired components and the output samples remain the same as obtained by convolution method, down-sampling by 2 is required in each branch.
Predict: Generate the prediction residual d[n] as the error in predicting odd samples from even input samples using predictor P.
Update: The coarse approximation c[n] is accomplished by applying an update operator U to d[n] and adding to even input samples.
The CDF (5,3) wavelet filter has the following coefficients:
Lowpass: (-1/8, 2/8 ,6/8 ,2/8, -1/8);
Highpass: (-1/2, 1, -1/2).
The polyphase matrix of the filter is:

$$P_1(z) = \begin{bmatrix} -\frac{1}{8}z + \frac{6}{8} - \frac{1}{8}z^{-1} & \frac{2}{8} + \frac{2}{8}z \\ -\frac{1}{2} - \frac{1}{2}z^{-1} & 1 \end{bmatrix} \quad (1)$$

The Split stage is given by factorization of the polyphase matrix

$$P_1(z) = \begin{bmatrix} 1 & 0.25(1+z) \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -0.5(1+z^{-1}) & 1 \end{bmatrix} \quad (2)$$

The predict step can be interpreted by following equation

$$y_{2i+1} = x_{2i+1} - 0.5(x_{2i} + x_{2i+2}), \quad (3)$$

The update step can be interpreted by following equation

$$y_{2i} = x_{2i} + 0.25(y_{2i+1} + y_{2i-1}) \quad (4)$$

Where x_{2k} and x_{2k+1} are the even and odd input samples and y_{2k+1} and y_{2k} represent the low and the high output coefficients respectively [22].

B. VLSI Architecture

The basic architecture of (5,3) is implemented in [14], [21] and [16]. [14] provides the conventional lifting based design of 2D DWT, as shown in Fig. 1. It consists of two stages of 1-D DWT, each stage having different length of delay element R(n). In the first stage (the Row processor), R(n) represents one delay element while in the second stage (the column processor), R(n) is N delays where N is the number of pixels in each row of the original image, as shown in Fig. 2. The input image $(N \times N)$ is fed to the architecture pixel by pixel using row by row scanning. In each clock cycle, a single pixel is fed. In the row processor, 1-D DWT of each row is computed to yield the low and high frequency components of each row. Then the column processor computes full set of 2-D DWT components; low-low (LL), low-high (LH), high-low (HL) and high-high (HH).

In the row processor, the input stream is split into odd and even streams, then predict and update stages follow. The pixels that take part in the computation of present output y[n] are x[n], x[n-1], x[n-2], x[n-3], and x[n-4]. Hence four delay elements are needed here. Similarly, in the column processor, five pixels from a single column are to be accessed for computation, so four row buffers (R(n) = N) are to be used.

III. Proposed Architecture

Timing refers to the logic delays between sequential elements. When a design does not meet timing, we mean that the delay of the critical path, that is, the largest delay between flip-flops (composed of combinatorial delay, clk-to-out delay, routing delay, setup timing, clock skew, and so on) is greater than the target clock period. In other words, the critical path delay sets upper limit on the clock frequency of a design. The standard metrics for timing are clock period and frequency [23].

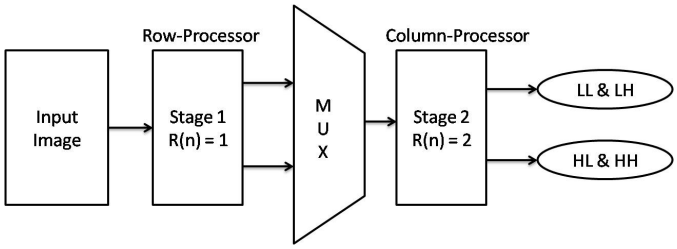


Fig. 1. Single level 2D CDF (5,3) DWT

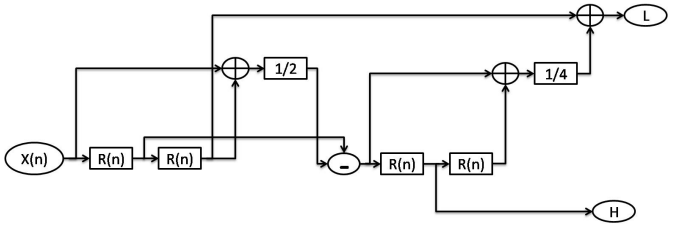


Fig. 2. 1-D DWT processor (Row or Column)

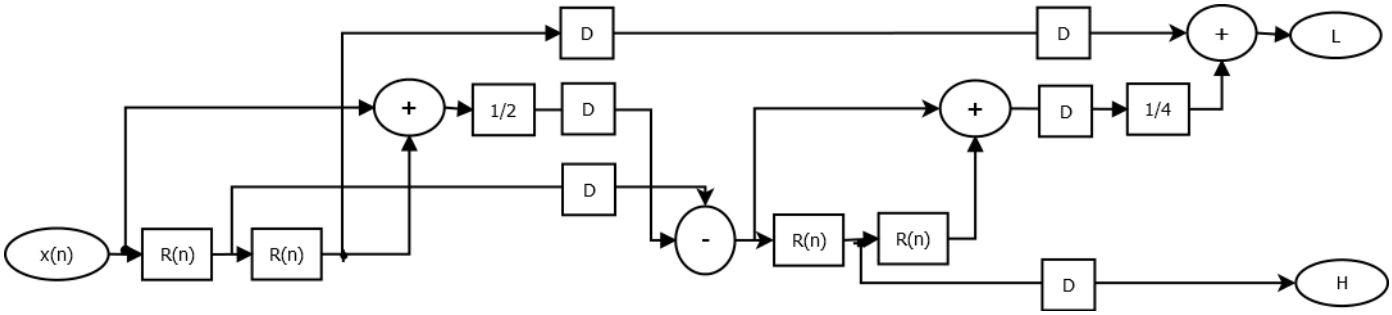


Fig. 3. Proposed 1-D DWT processor (row or column)

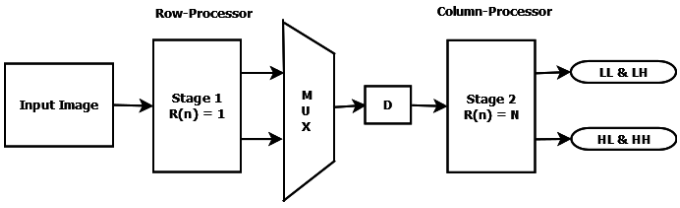


Fig. 4. Proposed single level 2-D CDF (5,3) DWT

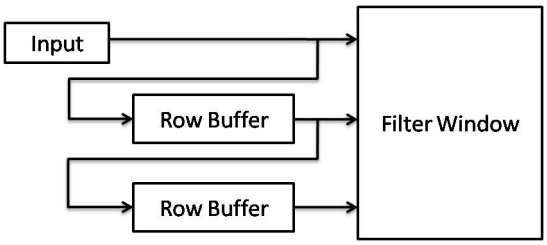


Fig. 5. Stream process filtering

Two types of optimizations are proposed in this paper:

1) Pipeline retimed architecture:
2) Unfolding retimed architecture:

A. Pipeline retimed architecture

The latency of the conventional structure is $2N + 2$ which means 1026 clock cycles for 512×512 image or 2050 clock cycles for an image of size 1024×1024. A small increase of 5 more clock cycles will have no effect on overall latency. But this will definitely help in optimization of timing. In order to increase the clock frequency, the critical path delay has to be minimized [23], [24]. The conventional implementation had a critical path delay of 8 adders and 4 multipliers, which will definitely needs to be minimized. [25] has provided two algorithms to check the feasibility of pipelining for obtaining a reduced clock period. Using Floyd-Warshall algorithm, we find that there is a feasibility of reducing the clock period. Now the pipelined architecture is obtained by cutset technique, in which a set of edges is removed from the signal flow graph in such a way that it creates two disconnected subgraphs. Then, a delay element is added in each of these edges. The resulting 2-D DWT for reduced clock period is shown in Fig. 4, with its 1-D DWT processor shown in Fig. 3.

As is evident from the Fig. 3, we have inserted delays in the cut-set tree so that the combinational critical path be evenly or near evenly divided. Now the critical path is 2 adders or 1 adder and 1 shifter. We can say the critical path has been reduced from $8T_A + 4T_M$ to $2T_A$ or $T_A + T_S$, where T_A, T_M and T_S are the computation times of adder, multiplier and shifter. The implementation results show that the minimum critical path delay has reduced from 13.566 ns to 3.01 ns, which is fourfold decrease in critical path delay. Conversely we can say that the proposed architecture is four times faster.

B. Unfolding retimed architecture

The filter function and the clock speed of the architecture are fixed to their optimal levels so far. We need to improve its throughput and latency, which can be accomplished by simultaneously processing multiple adjacent rows [26]. This requires multiple pixels to be input per clock cycle and exploits the fact that the windows for vertically adjacent outputs overlap significantly, as can be seen in Fig. 5 and Fig. 6. This is partially unrolling the vertical scan loop through the image. Note that the number of row buffers is unchanged. For an unroll factor of k (processing k rows of pixels in parallel) the combined window size is $W \times (W + k - 1)$. Of this, k rows of data are streamed in from input in parallel, so the remaining W-1 rows must come from row buffers. These buffers are arranged with a pitch of k rather than simply being chained. The parallel implementation will require k copies of

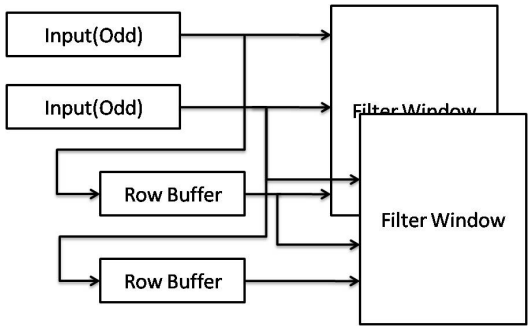


Fig. 6. Unfolded structure

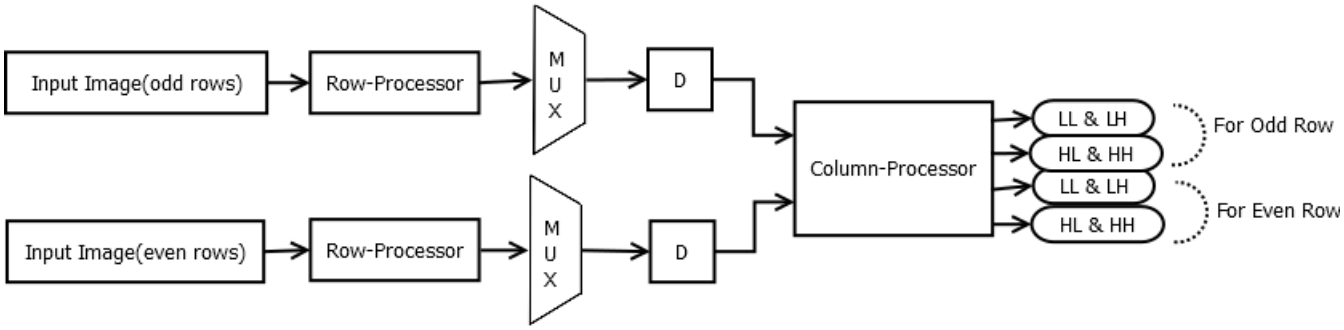


Fig. 7. Unfolded structure of 2-D DWT

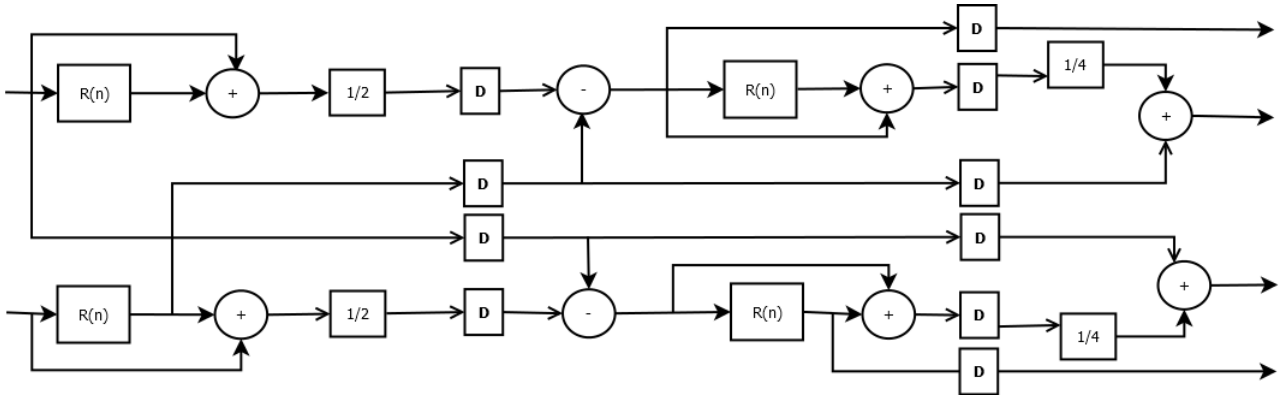


Fig. 8. Unfolded column-processor architecture

the filter function. However, with some filters, the overlap in windows can even enable some of the filter function logic to be shared [27], reducing the resource requirements further. Our case corresponds to k = 2, so two parallel inputs will scan the image in alternate manner, one input scanning the odd rows of the image in pixel by pixel manner while other scanning the even rows of the input image.

Here two rows (even and odd) are processed in parallel with resources shared between the two parallel branches. The actual implementation is shown in Fig. 7, with column processor architecture as shown in Fig. 8. It is evident from Fig. 8 that two transformed coefficients are output in each clock cycle, so throughput is improved and reaches twice its initial value. Also now the output latency has been reduced to $N + 7$.

1) Multiplier Design: Multiplication in binary can be represented as a series of addition and shift operations. Usually multiplication requires more logic and computation time than addition. So, it is always a good practice to minimize the use of multipliers in hardware designs. Here, we have multiplication with the coefficients having values 0.5 and 0.25, which can be easily obtained using shift operations. Multiplication of the input with $0.5(= 2^{-1})$ and $0.25(= 2^{-2})$ requires the input to be shifted right by one and two bits respectively.

IV. Implementation Results

We have proposed two 2-D DWT architectures of CDF (5,3) in this paper. The structures are synthesized on 6VLX760FF1760-2 Xilinx FPGA platform. The word length is set to 16 bit using signed arithmetic operations, while evaluating the design. The architecture is designed for image size of 512×512 and can be easily extended for any even-sized image without modifying much. Also the hardware can be easily replicated for J number of levels. Zero padding is used for the computation of the whole image, in order to take care of the filter effects on image boundary. The architecture of [14] is also implemented alongside our proposed architectures to reflect the optimizations made therein. The comparison of resource utilization and timing is made in table I and table II. It is evident from table I that the hardware requirements of the proposed architecture has increased but the cost to be paid for the extra hardware is much less compared to the high performance achieved from the proposed design, as shown in table II.

It should be noted that the maximum clock frequency of the pipeline retimed architecture has drastically improved by minimizing the critical path delay. This has cost as many as 13 additional delay elements in total, maximum of five delays in feed-forward path i.e. five more additional latency cycles. The register balancing option available in Xilinx ISE has reduced four delay registers without affecting any other parameter. The unfolded retimed architecture has paralleled the pipeline retimed architecture to yield twice the throughput and half the output latency, by doubling the filter function, without any addition to the row buffers. So unfolded retimed architecture provides optimized throughput, reduced latency as well as optimized clock frequency design. In table III, the performance of the proposed architecture is compared with other existing efficient architectures. It is evident that our

TABLE I
SYNTHESIS RESULTS FOR HARDWARE UTILIZATION OF 2D CDF 5/3 DWT ARCHITECTURE AND COMPARISON WITH EXISTING ARCHITECTURE (J: NUMBER OF DWT LEVELS)

Architecture	Adders/Subtracters	Multipliers/Shifters	Registers	Slice Registers	Slice LUTs	IOBs	Control Complexity
Al_Azawi [14]	8J	4J	4N + 4	359	368	26	Simple
Proposed pipelined architecture	8J	4J	4N + 13	411	361	26	Simple
Proposed unfolded architecture	16J	8J	4N + 25	511	433	50	Medium

TABLE II
TIMING PERFORMANCE COMPARISON OF 2D CDF 5/3 DWT ARCHITECTURE WITH EXISTING ARCHITECTURE

Architecture	Output Latency (clock cycles)	Computation Time (clock cycles)	Critical Path (combinational logic delay)	Critical Path Delay (ns)	Minimum Clock Period (ns)	Throughput (samples per clock cycle)
Al_Azawi [14]	$2N+2$	N^2+2N+2	$8T_A+4T_M$	13.566	5.930	1
Proposed pipe_arch	$2N+7$	N^2+2N+7	$2T_A$ OR T_A+T_S	3.010	2.228	1
Proposed unfold_arch	$N+7$	$N^2/2+N+7$	$2T_A$ OR T_A+T_S	3.040	2.228	2

TABLE III
HARDWARE AND TIMING PERFORMANCE COMPARISON AMONG DIFFERENT EXISTING 2D CDF 5/3 DWT ARCHITECTURES

Architecture	Multipliers	Adders	Storage Size	Computation Time (clock cycles)	Output Latency (clock cycles)	Throughput (samples per clock cycle)	Critical Path (combinational delay)	Control Complexity
Wu [29]	16	16	$N^2/4$	$N^2/2$	2N	1	T_M+2T_A	Medium
Andra [7]	4	8	$N^2/4$	$N^2/2$	2N	1	T_M	Medium
Laio [30]	4	8	$6N$	N^2	2N	1	T_M+2T_A	Complex
Barua [17]	4	8	$N^2/4$	$N^2/2$	5N	1	–	Simple
Chengy (FA) [28]	4	8	$N^2/4$	$N^2/2$	N	1	T_M+2T_A	Simple
Chengy (HA) [28]	8	16	$N^2/4$	$N^2/4$	$N/2$	1	T_M+2T_A	Simple
Tian [31]	8	16	$N^2/2$	$N^2/2$	2N	2	T_M+2T_A	Simple
Al_Azawi [14]	4	8	$4N+4$	N^2+2N+2	$2N+2$	1	$4T_M+8T_A$	Simple
Proposed architecture	8	16	$4N+25$	$N^2/2+N+7$	$N+7$	2	$2T_A$ OR T_A+T_S	Medium

architecture is the only one that provides optimized throughput along with minimized clock period to such extent.

We have tested the implementation of the proposed architecture on several images of sizes 0.25 Megapixels (512×512), 5 Megapixels (2560×1920), 15 Megapixels (5184×2920) and 20 Megapixels (5184×3888). The computation time for the four image sizes are 0.397 ms, 5.84 ms, 16.86 ms and 22.50 ms respectively. The corresponding number of images that can be transformed per second are 2500, 171, 59 and 44 respectively.

V. Conclusion

In this paper, we have presented a high speed memory-efficient architecture that can convert images into their corresponding 2D-DWT coefficients at very high speed. The simulation results depict that approximately 4 rows of input image need to be stored in buffers for encoding an image. The proposed architecture can encode as many as 59 images, each of size 15 megapixels or 45 images, each of size 20 megapixels in approximately one second, making our architecture a potential candidate for video processing applications. Even higher resolution images can be transformed without affecting the video quality. Furthermore, the proposed architecture is quite simple and can be applied to images having even size.

References

[1] M. Vishwanath, R. Owens, and M. J. Irwin, "VLSI architectures for the discrete wavelet transform," *IEEE Trans. on Circuits Syst. II*, vol. 42, pp. 305-316, May 1995.

[2] K. K. Parhi and T. Nishitani,"VLSI architectures for discrete wavelet transforms," *IEEE Trans. on VLSI Systems*, vol. 1, pp. 191-202, June 1993.

[3] A. Grzeszczak, M. K. Mandal, S. Panchanathan, and T. Yeap,"VLSI implementation of discrete wavelet transform," *IEEE Trans. on VLSI Systems*, vol. 4, pp. 421-433, June 1996.

[4] C. Chakrabarti and M. Vishwanath, "Efficient realizations of the discrete and continuous wavelet transforms: From single chip implementations to mappings on SIMD array computers," *IEEE Trans. on Signal Processing*, vol. 43, pp. 759-771, March 1995.

[5] I. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting schemes," *J. Fourier Anal. Appl.*, vol. 4, no. 3, pp. 247-269, May 1998.

[6] W. Sweldens, "The lifting scheme: a custom-design construction of biorthogonal wavelets," *Applied and Computaional Harmonic Analysis*, vol. 3, no. 15, pp. 186-200, 1996.

[7] A. R. Calderbank, I. Daubechies,W. Sweldens, and B. L. Yeo, "Wavelet transforms that map integers to integers," *Applied Computational Harmonic Analysis*, vol. 5, pp. 332-369, July 1998.

[8] K. Andra, C. Chakrabarti and T. Acharya, "A VLSI Architecture for Lifting-Based Forward and Inverse Wavelet Transform," *IEEE Trans. on Signal Processing*, vol. 50, no. 4, April 2002.
[9] JPEG2000 verification model 8.5 (Technical Description), Sept 13, 2000.
[10] ITU-T Recommend. T.800-ISO FCD15444-1: JPEG2000 Image Coding System. International Organization for Standardization, ISO/IEC JTC1 SC29/WG1, 2000.
[11] M. Unser and T. Blu, "Mathematical Properties of the JPEG2000 Wavelet Filters," *IEEE Trans. on Image Processing*, vol. 12, no. 9, September 2003.
[12] W Wang, Z. Du and Y. Zong, "High-Speed FPGA Implementation for DWT of Lifting Scheme," *5th International Conference on Wireless Communications, Networking and Mobile Computing*, September 2009.
[13] U. Bhanu N and A. Chilambuchelvan, "A Detailed Survey on VLSI Architectures for Lifting based DWT for efficient hardware implementation," *International Journal of VLSI design & Communication Systems (VLSICS)*, vol.3, no.2, April 2012.
[14] S. Al-Azawi, Y. A. Abbas and R. Jidin, "Low Complexity Multidimensional CDF 5/3 DWT Architecture," *9th International Symposium on Communication Systems, Networks & Digital Sign (CSNDSP)*,2014.
[15] X. Fan, Z. Pang, D. Chen and H. Z. Tan, "A Pipeline Architecture for 2-D Lifting-based Discrete Wavelet Transform of JPEG2000," *International conference on Multimedia Technology*, October 2010.
[16] A. D. Darji, R. Bansal, S. N. Merchant and A. N. Chandorkar, "High Speed VLSI Architecture for 2-D Lifting Discrete Wavelet Transform," *Conference on Design and Architectures for Signal and Image Processing*, November 2011.
[17] S. Barua, J. E. Carletta, K. A. Kotteri and A. E. Bell, "An efficient architecture for lifting-based two-dimensional discrete wavelet transforms," *Integration, the VLSI journal*, vol. 38, pp. 341-352, 2005.
[18] W. Zhang, Z. Jiang, Z. Gao, and Y. Liu, "An Efficient VLSI Architecture for Lifting-Based Discrete Wavelet Transform," *IEEE Trans. on Circuits and SystemsII: Express Briefs*, vol. 59, no. 3, March 2012.
[19] V. Gupta and K. Raj, "An Efficient Modified Lifting Based 2-D Discrete Wavelet Transform Architecture," *1st International Conference on Recent Advances in Information Technology*, 2012.
[20] T. S. M. Atri, Y. Said and R. Tourki, "Real Time FPGA acceleration for Discrete Wavelet Transform of the 5/3 Filter for JPEG 2000," *6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, 2012.
[21] C. Desmouliers, E. Oruklu and J. Saniie, "Discrete wavelet transform realisation using run-time reconfiguration of field programmable gate array (FPGA)s," *IET Circuits Devices Syst.*, vol. 5, no. 4, pp. 321-328, 2011.
[22] N. Sriram and R. Shyamsunder, "3-D medical image compression using 3-D wavelet coders," emphDigital Signal Processing, vol. 21, pp. 100-109, 2011.
[23] S. Kilts, "Advanced FPGA Design Architecture, Implementation, and Optimization," *John Wiley & Sons, Inc., Hoboken, New Jersey*, 2007.
[24] D. G. Bailey, "Design for Embedded Image Processing on FPGAs," *John Wiley & Sons (Asia) Pvt. Ltd.*, 2011.
[25] K. K. Parhi, "VLSI Digital Signal Processing Systems: Design and Implementation," *John Wiley & Sons (New York) Pvt. Ltd.*, 1999.
[26] B. A. Draper, J. R. Beveridge, A. P. W. Bohm, C. Ross, M. Chawatche and J. Hammes, "Accelerated image processing on FPGAs," *IEEE Trans. on Image Processing*, 2003.
[27] L. E. Lucke and K. K. Parhi "Parallel structures for rank order and stack filters," *IEEE International Conference on Acoustics, Speech and Signal Processing*, San Francisco, California, USA, vol. 5, March, 1992.
[28] C. Xiong, J. Tian, and J. Liu, "Efficient Architectures for Two-Dimensional Discrete Wavelet Transform Using Lifting Scheme," *IEEE Trans. on Image Processing*, vol. 16, no. 3, March 2007.
[29] P. C. Wu and L. G. Chen, "An Efficient Architecture for Two-Dimensional Discrete Wavelet Transform," *IEEE Trans. on Circuits and Systems for Video Technology*,vol. 11, no. 4, April 2001.
[30] H. Liao, M. Kr. Mandal and B. F. Cockburn, "Efficient Architectures for 1-D and 2-D Lifting-Based Wavelet Transforms," *IEEE Trans. on Signal Processing*, vol. 52, no. 5, May 2004.
[31] X. Tian, L. Wu, Y.-H. Tan, and J.-W. Tian, "Efficient Multi-Input/Multi-Output VLSI Architecture for Two-Dimensional Lifting-Based Discrete Wavelet Transform," *IEEE Trans. on Computers*, vol. 60, no. 8, August 2011.

Decoupling of Broadband Optical MIMO Systems Using the Multiple Shift SBR2 Algorithm

Zeliang Wang, André Sandmann, John G. McWhirter and Andreas Ahrens

***Abstract*—Polynomial singular value decomposition (PSVD) plays a very important role in broadband multiple-input multiple-output (MIMO) systems. One of its applications lies in the decoupling of MIMO convolutive mixing channel matrix in order to recover the transmitted signals corrupted by the channel interference (CI) at the receiver. In this paper, a novel algorithm, known as multiple shift second order sequential best rotation (MS-SBR2), is proposed to compute the approximate PSVD of the broadband MIMO channel matrix. Experimental examples, including a measured (2×2) optical MIMO channel impulse response using the multi-mode fiber (MMF) testbed, are presented to examine the proposed algorithm. Bit error rate (BER) performances are evaluated among different transmission schemes. In addition, power allocation (PA) schemes are investigated to further optimize the BER performance.**

***Keywords*—Multiple shift SBR2, polynomial SVD, precoding, equalization, multi-mode fiber, optical MIMO systems, power allocation.**

I. Introduction

An explosive development of MIMO technology has been witnessed in wireless communication systems over the last decade. Compared to single-input single-output (SISO) systems, MIMO systems are capable of achieving higher data rates and transmission reliabilities by using the techniques of spatial multiplexing and transmit diversity. Aiming to increase the fiber capacity, the concept of MIMO in optical transmission systems has also attracted intensive research interests [1], [2].

Due to the multipath effect in broadband MIMO systems, the channel is characterized by frequency-selective fading, so apart from the channel interference caused by the MIMO components, there also exists inter-symbol interference (ISI) between the transmit symbols. Provided the approximate channel length is known at the transmitter, a standard approach of combating the ISI is to use multi-carrier modulation techniques, such as orthogonal frequency division multiplexing (OFDM) with cyclic prefix which can divide the spectrum into a number of narrowband channels. In other words, the frequency-selective or broadband MIMO channel is turned into a set of parallel frequency-flat or narrowband MIMO channels where the ISI does not exist anymore, and each narrowband channel can be independently addressed using existing narrowband optimal techniques. This type of MIMO-OFDM system was well implemented by a spatio-temporal vector coding (STVC) [3], [4] communication structure combined with the singular value decomposition (SVD) based equalization technique [5]. Another widely applied approach is based on optimal filter bank transceiver techniques [6] which involve block processing and guard intervals to eliminate inter-block interference (IBI). These two traditional techniques are in common in the sense of eliminating the polynomial nature of the channel which corresponds to the IBI due to the time-dispersive nature of the channel, and essentially they are all designed to convert the broadband problem into narrowband ones.

Manuscript received October 30, 2016; revised March 30, 2017.

Z. Wang and J. G. McWhirter are with the School of Engineering, Cardiff University, Cardiff CF24 3AA, Wales, UK (e-mail: wangz49@cardiff.ac.uk, mcwhirterjg@cardiff.ac.uk).

A. Sandmann and A. Ahrens are with Hochschule Wismar, University of Applied Sciences: Technology, Business and Design, Philipp-Müller-Straße 14, 23966 Wismar, Germany (e-mail: andre.sandmann@hs-wismar.de, andreas.ahrens@hs-wismar.de).

II. The State of the Art

The work which we present here is related with the broadband MIMO decoupling method proposed in [7], [8]. This method is essentially distinct from the traditional techniques like OFDM or optimal filter bank transceiver, as it can be applied to decouple the broadband (polynomial) MIMO channel directly, instead of converting it into narrowband channels. It mainly consists of two steps. The first step is based on the PSVD that was used to diagonalize the broadband MIMO channel matrix in order to remove the CI, which results in the frequency-selective MIMO channel decoupled into a number of independent frequency-selective SISO channels. The second step involves removing the remaining inter-symbol interference (ISI) for each SISO channel, which can be implemented by further equalization techniques, such as zero-forcing equalization or maximum likelihood sequence estimations (MLSE).

There are different ways of calculating the PSVD of a polynomial matrix, such as using polynomial matrix QR decomposition to formulate the PSVD [9], PSVD based on generalized Kogbetliantz transformations [10], and PSVD by polynomial matrix eigenvalue decomposition (PEVD) method [11], which is analogous to how the scalar matrix eigenvalue decomposition (EVD) can be used to generate the singular value decomposition (SVD) of a matrix. In terms of the PSVD by PEVD method, the second order sequential best rotation (SBR2) algorithm [12] has been used in the existing literatures. However, an improved version of the SBR2 algorithm, i.e. MS-SBR2 [13], has been recently proposed by the authors for calculating the PEVD of polynomial matrices. The improved algorithm can provide much faster convergence than the SBR2 algorithm when dealing with high dimension polynomial matrices. In other words, the diagonalization of bigger MIMO

channel matrices can be implemented faster than that of using the SBR2 algorithm.

The main contributions of this work are the exploitation of the proposed PSVD by MS-SBR2 method in the application of solving the broadband MIMO decoupling problem, comparisons against the PSVD by SBR2 method, the discussion of the accuracy of the PSVD approach. The results presented in this paper include a simulated broadband channel matrix example which is designed to test how the PSVD method works. More importantly, a (2×2) optical MIMO channel which comprises a 1.4 km MMF and optical couplers at both ends is designed to examine the BER performance of a optical MIMO system in which the channel impulse responses are measured for the operating wavelength of 1576 nm [8]. In particular, transmission and power allocation schemes are employed to bring further improvement with respect to the BER performance.

The remaining parts of the paper are structured as follows. The convolutive MIMO channel model with polynomial matrix representation is described in Sec. III. In Sec. IV we introduce the idea of broadband MIMO channel decomposition, i.e. PSVD. Sec. V presents the proposed MS-SBR2 algorithm for calculating the PSVD. Simulation results and conclusions are shown in Sec. VI and Sec. VII, respectively.

III. MIMO Convolutive Mixing Model

Given a frequency selective MIMO link with n_{T} inputs and n_{R} outputs, the convolutive mixing channel can be modelled as a polynomial matrix with an indeterminate variable z^{-1} given by

$$\underline{\mathbf{C}}(z) = \sum_{\tau=0}^{T} \mathbf{C}[\tau] z^{-\tau} = \begin{bmatrix} \underline{c}_{11}(z) & \cdots & \underline{c}_{1n_{\mathrm{T}}}(z) \\ \vdots & \ddots & \vdots \\ \underline{c}_{n_{\mathrm{R}}1}(z) & \cdots & \underline{c}_{n_{\mathrm{R}}n_{\mathrm{T}}}(z) \end{bmatrix}, \quad (1)$$

where $\tau, T \in \mathbb{Z}$ and $\mathbf{C}[\tau] \in \mathbb{C}^{n_{\mathrm{R}} \times n_{\mathrm{T}}}$ denotes the polynomial coefficient matrix at time lag τ and $\underline{c}_{\nu\mu}(z)$, $\nu \in \{1, 2, \cdots, n_{\mathrm{R}}\}$, $\mu \in \{1, 2, \cdots, n_{\mathrm{T}}\}$, is the polynomial matrix entity which represents the channel impulse response between the μ-th input and the ν-th output. It takes the form of

$$\underline{c}_{\nu\mu}(z) = \sum_{\tau=0}^{T} c_{\nu\mu}[\tau] z^{-\tau}, \quad (2)$$

where $c_{\nu\mu}[\tau]$ denotes a non-zero element of the symbol rate sampled overall channel impulse response at the τ-th lag. In this case there are $T+1$ lags in total for each SISO channel. Throughout this paper, polynomial matrices and vectors are denoted as underscored boldface letters.

In the context of optical MIMO systems, it should be noticed that the group delays in a MMF optical channel belong to a fixed set of values in contrast with that of the wireless channel which can change from one realisation to another [14]. Assuming that the transmit signal is represented by $\underline{\mathbf{s}}'(z)$, the convolutively mixed received signal $\underline{\mathbf{x}}'(z)$ can be expressed as

$$\underline{\mathbf{x}}'(z) = \underline{\mathbf{C}}(z)\underline{\mathbf{s}}'(z) + \underline{\mathbf{n}}(z), \quad (3)$$

where $\underline{\mathbf{n}}(z)$ represents the additive noise which has variance of $\sigma^2 \mathbf{I}_{n_{\mathrm{R}}}$.

IV. Broadband MIMO Channel Decomposition via PSVD

One potential application of PSVD is to enable communication over a broadband MIMO system in which the channel matrix is represented by a polynomial matrix as shown in (1). In this case, provided the channel matrix has firstly been estimated, the PSVD then can be used to simplify a MIMO channel equalization problem into a set of independent SISO problems. In other words, the CI can be removed by performing the PSVD to the channel matrix $\underline{\mathbf{C}}(z)$, which can be expressed as [11]

$$\underline{\mathbf{C}}(z) = \widetilde{\underline{\mathbf{U}}}(z)\underline{\mathbf{\Sigma}}(z)\underline{\mathbf{V}}(z) = \widetilde{\underline{\mathbf{U}}}(z) \begin{bmatrix} \underline{\mathbf{\Gamma}}(z) \\ 0 \end{bmatrix} \underline{\mathbf{V}}(z), \quad (4)$$

where we assume $n_{\mathrm{R}} \geq n_{\mathrm{T}}$, and $\underline{\mathbf{\Gamma}}(z)$ is a diagonal polynomial matrix with $n = n_{\mathrm{T}}$ diagonal elements, i.e. $\underline{\mathbf{\Gamma}}(z) = \mathrm{diag}\{\underline{\gamma}_{11}(z), \underline{\gamma}_{22}(z), \cdots, \underline{\gamma}_{nn}(z)\}$. $\widetilde{\underline{\mathbf{U}}}(z)$ and $\underline{\mathbf{V}}(z)$ are paraunitary polynomial matrices with dimension $n_{\mathrm{R}} \times n_{\mathrm{R}}$ and $n_{\mathrm{T}} \times n_{\mathrm{T}}$ respectively, such that $\widetilde{\underline{\mathbf{U}}}(z)\underline{\mathbf{U}}(z) = \underline{\mathbf{U}}(z)\widetilde{\underline{\mathbf{U}}}(z) = \mathbf{I}_{n_{\mathrm{R}}}$ and $\widetilde{\underline{\mathbf{V}}}(z)\underline{\mathbf{V}}(z) = \underline{\mathbf{V}}(z)\widetilde{\underline{\mathbf{V}}}(z) = \mathbf{I}_{n_{\mathrm{T}}}$. Here the notation $\{\widetilde{\ }\}$ over a polynomial matrix denotes the paraconjugate operation which is computed by performing Hermitian transpose $\{\cdot\}^{\mathrm{H}}$ to all the polynomial coefficient matrices $\mathbf{U}[\tau]$ and time-reversing all entries inside, i.e. $\widetilde{\underline{\mathbf{U}}}(z) = \underline{\mathbf{U}}^{\mathrm{H}}(1/z)$.

Note that $\widetilde{\underline{\mathbf{U}}}(z)$ and $\underline{\mathbf{V}}(z)$ are acting as the multichannel all-pass filters which can transform the frequency selective MIMO channel into a number of independent frequency selective SISO channels while still preserving the total signal energy [15]. In this paper, the PSVD in (4) is implemented by calculating the PEVD of two para-Hermitian polynomial matrices $\underline{\mathbf{C}}(z)\widetilde{\underline{\mathbf{C}}}(z)$ and $\widetilde{\underline{\mathbf{C}}}(z)\underline{\mathbf{C}}(z)$, which take the form as

$$[\underline{\mathbf{C}}(z)\widetilde{\underline{\mathbf{C}}}(z)]_{n_{\mathrm{R}} \times n_{\mathrm{R}}} = \widetilde{\underline{\mathbf{U}}}(z)\underline{\mathbf{\Sigma}}(z)\widetilde{\underline{\mathbf{\Sigma}}}(z)\underline{\mathbf{U}}(z), \quad (5)$$

and

$$[\widetilde{\underline{\mathbf{C}}}(z)\underline{\mathbf{C}}(z)]_{n_{\mathrm{T}} \times n_{\mathrm{T}}} = \widetilde{\underline{\mathbf{V}}}(z)\widetilde{\underline{\mathbf{\Sigma}}}(z)\underline{\mathbf{\Sigma}}(z)\underline{\mathbf{V}}(z). \quad (6)$$

Further details about the PEVD algorithms will be discussed in the following section. To eliminate the CI, the source signal $\underline{\mathbf{s}}(z)$ is filtered by the paraunitary transformation matrix $\widetilde{\underline{\mathbf{V}}}(z)$ at the transmitter, i.e. $\underline{\mathbf{s}}'(z) = \widetilde{\underline{\mathbf{V}}}(z)\,\underline{\mathbf{s}}(z)$, and the received signal $\underline{\mathbf{x}}'(z)$ is pre-multiplied by $\underline{\mathbf{U}}(z)$ such that $\underline{\mathbf{x}}(z) = \underline{\mathbf{U}}(z)\,\underline{\mathbf{x}}'(z)$ at the receiver, which results in

$$\underline{\mathbf{x}}(z) = \underline{\mathbf{\Sigma}}(z)\underline{\mathbf{s}}(z) + \underline{\mathbf{w}}(z), \quad (7)$$

where $\underline{\mathbf{w}}(z) = \underline{\mathbf{U}}(z)\underline{\mathbf{n}}(z)$. Note that neither the transmit power is increased, nor the channel noise is enhanced here.

Unlike the conventional SVD-based method, each diagonal element (also called layer) in $\underline{\mathbf{\Sigma}}(z)$ is frequency-selective and hence ISI occurs. In order to remove the ISI, layer-specific T-spaced zero forcing equalizers [8] are adopted in this paper and therefore this equalization scheme is entitled T-PSVD. A block diagram of the proposed communication system can be depicted in Fig. 1.

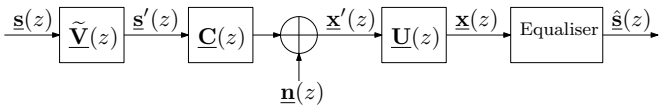


Fig. 1. Block diagram of the proposed communication system using the PSVD.

V. PSVD USING THE MS-SBR2 ALGORITHM

As mentioned above, the PEVD method can be used to formulate the PSVD problem in (4), and the idea of PEVD has been generalized as [12]

$$\underline{\mathbf{H}}(z)\underline{\mathbf{R}}(z)\widetilde{\underline{\mathbf{H}}}(z) \approx \underline{\mathbf{D}}(z), \tag{8}$$

where $\underline{\mathbf{R}}(z) \in \mathbb{C}^{M\times M}$ is a para-Hermitian matrix, such that $\widetilde{\underline{\mathbf{R}}}(z) = \underline{\mathbf{R}}(z)$. $\underline{\mathbf{H}}(z)$ is a paraunitary matrix which aims to diagonalize $\underline{\mathbf{R}}(z)$ by means of paraunitary similarity transformation, and $\underline{\mathbf{D}}(z)$ is (ideally) a diagonal matrix. The approximation sign in (8) indicates that a PEVD does not necessarily exist if the paraunitary matrix $\underline{\mathbf{H}}(z)$ only contains FIR components. However it has been proved that a very close approximation can be achieved by letting the polynomial order of $\underline{\mathbf{H}}(z)$ grow arbitrarily large [16]. This is an iterative process which transforms all the off-diagonal elements in $\underline{\mathbf{R}}(z)$ onto the diagonal. Several algorithms [12], [17], [18] exist for calculating the PEVD, however, this paper is concerned only with the MS-SBR2 algorithm previously presented by the authors in [13].

The MS-SBR2 algorithm is an improved version of the SBR2 algorithm in terms of the algorithm convergence speed. Basically it adopts the advantages of less computational cost from SBR2 and the faster convergence from MSME-SMD [18], which seems to provide a compromise between the SBR2 and the SMD algorithm family. For the following part of this section, the SBR2 algorithm is firstly introduced before we move forward to the MS-SBR2 algorithm, and a numerical example is chosen to assess the performance of the algorithms, and then followed by a discussion of the computational accuracy.

A. Second Order Sequential Best Rotation (SBR2) Algorithm

The SBR2 algorithm was designed to iteratively eliminate the off-diagonal elements for para-Hermitian matrices by using the paraunitary similarity transformations shown in (8). At the i-th iteration, the SBR2 algorithm [12] starts by locating the maximum off-diagonal element $r_{jk}^{(i)}[\tau]$. To find the maximum off-diagonal element, we define a matrix $\mathbf{S}^{(i)}[\tau]$, which contains only the upper triangular elements in $\mathbf{R}^{(i-1)}[\tau]$ with the remaining elements set to zero. Thus the location of $r_{jk}^{(i)}[\tau]$, $(j<k)$ found at i-th iteration satisfies

$$\{j^{(i)}, k^{(i)}, \tau^{(i)}\} = \arg\max_{j,k,\tau} \|\mathbf{S}^{(i)}[\tau]\|_\infty, \tag{9}$$

where $j^{(i)}$, $k^{(i)}$ and $\tau^{(i)}$ are the corresponding row, column and time lag index. An elementary delay matrix $\underline{\mathbf{P}}^{(i)}(z)$ and Jacobi rotation $\mathbf{Q}^{(i)}$ are sequentially applied to bring $r_{jk}^{(i)}[\tau]$ and its complex conjugate $r_{kj}^{(i)}[-\tau]$ onto the zero-lag ($\tau=0$)

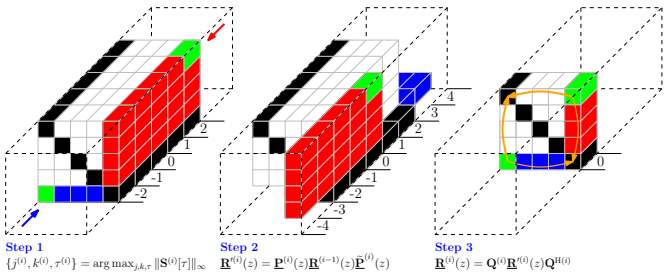


Fig. 2. A 3-dimensional illustration of a 5×5 polynomial matrix example, showing the i-th iteration process using SBR2; Assuming the maximum off-diagonal element $r_{jk}^{(i)}[\tau]$ found is at the location of $\{1,5,2\}$ represented in green color, step 1 shows the location information; Step 2 describes the corresponding row and column shift operations; Step 3 is to transfer the pairwise maximum elements $r_{jk}^{(i)}[\tau]$ and $r_{kj}^{(i)}[-\tau]$ onto diagonal (only zero-lag coefficient matrix is shown here for visibility purpose) [12], [18].

coefficient matrix $\mathbf{R}^{(i-1)}[0]$, and then rotate its energy onto the diagonal. This results in $\underline{\mathbf{R}}^{(i)}(z)$ given by

$$\underline{\mathbf{R}}^{(i)}(z) = \mathbf{Q}^{(i)}\underline{\mathbf{P}}^{(i)}(z)\underline{\mathbf{R}}^{(i-1)}(z)\widetilde{\underline{\mathbf{P}}}^{(i)}(z)\mathbf{Q}^{\mathrm{H}(i)}, \tag{10}$$

where $\underline{\mathbf{P}}^{(i)}(z)$ is expressed as

$$\underline{\mathbf{P}}^{(i)}(z) = \mathrm{diag}\,\{\underbrace{1,\cdots,1}_{k^{(i)}-1}, z^{-\tau^{(i)}}, \underbrace{1,\cdots,1}_{M-k^{(i)}}\}. \tag{11}$$

A 3-dimensional illustration which shows the procedure of the i-th iteration in SBR2 is described in Fig. 2. Thus the elementary paraunitary matrix $\underline{\mathbf{E}}^{(i)}(z)$ can be expressed as

$$\underline{\mathbf{E}}^{(i)}(z) = \mathbf{Q}^{(i)}\underline{\mathbf{P}}^{(i)}(z). \tag{12}$$

The algorithm continues its iterative process until all the off-diagonal elements in $\underline{\mathbf{R}}^{(i)}(z)$ are smaller than a given threshold ϵ which can be set to a very small value to achieve sufficient accuracy. Assuming that the algorithm has converged at the N-th iteration, the diagonalized para-Hermitian matrix in (8) takes the form of

$$\underline{\mathbf{D}}(z) = \mathrm{diag}\,\{\underline{d}_{11}(z), \underline{d}_{22}(z), \cdots, \underline{d}_{MM}(z)\}, \tag{13}$$

and the generated paraunitary polynomial matrix is given by

$$\underline{\mathbf{H}}(z) = \prod_{i=1}^{N} \underline{\mathbf{E}}^{(i)}(z) = \underline{\mathbf{E}}^{(N)}(z)\cdots\underline{\mathbf{E}}^{(2)}(z)\underline{\mathbf{E}}^{(1)}(z). \tag{14}$$

B. Multiple Shift SBR2 (MS-SBR2) Algorithm

The MS-SBR2 algorithm uses a distinguishing search strategy of the off-diagonal elements which is akin to that of the MSME-SMD algorithm, so that it can achieve the diagonalization with less iterations than the SBR2 algorithm. For the i-th iteration, the MS-SBR2 algorithm involves multiple shifts operations $\widehat{\underline{\mathbf{P}}}^{(i)}(z)$, followed by a sequence of Jacobi rotations $\widehat{\mathbf{Q}}^{(i)}$. Therefore the resulting para-Hermitian matrix is computed by

$$\underline{\mathbf{R}}^{(i)}(z) = \widehat{\mathbf{Q}}^{(i)}\widehat{\underline{\mathbf{P}}}^{(i)}(z)\underline{\mathbf{R}}^{(i-1)}(z)\widetilde{\widehat{\underline{\mathbf{P}}}}^{(i)}(z)\widehat{\mathbf{Q}}^{\mathrm{H}(i)}, \tag{15}$$

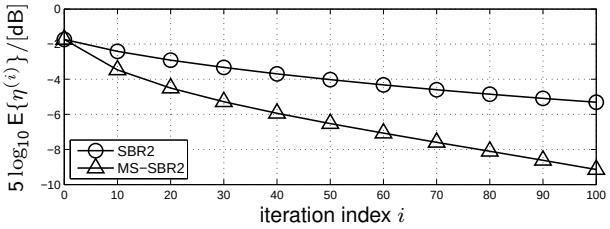


Fig. 3. Comparison of normalized off-diagonal energy $\eta^{(i)}$ between SBR2 and MS-SBR2 algorithms, showing ensemble averages versus iterations.

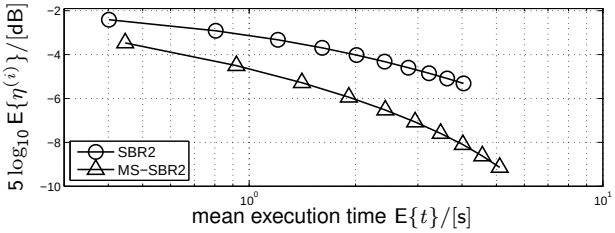


Fig. 4. Comparison of normalized off-diagonal energy $\eta^{(i)}$ between SBR2 and MS-SBR2 algorithms, showing ensemble averages versus mean execution time (measured in MATLAB R2014a on a PC with configurations Intel Core i7-3770T CPU@2.50 GHz and 16 GB RAM).

where $\widehat{\underline{\mathbf{P}}}^{(i)}(z) = \prod_{l=1}^{L^{(i)}} \underline{\mathbf{P}}^{(l,i)}(z)$, $\widehat{\mathbf{Q}}^{(i)} = \prod_{l=1}^{L^{(i)}} \mathbf{Q}^{(l,i)}$ and $L^{(i)}$ denotes the total number of off-diagonal elements shifted to the zero-lag coefficient matrix at the i-th iteration ($L^{(i)} \in \mathbb{Z},\ 1 \leq L^{(i)} \leq \lfloor M/2 \rfloor$). Accordingly the delay matrix at the l-th delay stage within i-th iteration is represented by

$$\underline{\mathbf{P}}^{(l,i)}(z) = \mathrm{diag}\{\underbrace{1, \cdots, 1}_{k^{(l,i)}-1}, z^{-\tau^{(l,i)}}, \underbrace{1, \cdots, 1}_{M-k^{(l,i)}}\}, \qquad (16)$$

and the elementary paraunitary matrix can be expressed as $\widehat{\underline{\mathbf{E}}}^{(i)}(z) = \widehat{\mathbf{Q}}^{(i)}\widehat{\underline{\mathbf{P}}}^{(i)}(z)$. Note that when $L^{(i)} = 1$, the MS-SBR2 algorithm is identical to the SBR2 algorithm.

Another motivation of introducing the multiple shift idea into the SBR2 algorithm is that it permits us to minimize the order growth of polynomial matrices by making all row (column) shifts in the same direction, which can potentially reduce the computational cost of the algorithm [19]. The PEVD algorithms are assessed in terms of the normalized off-diagonal energy $\eta^{(i)}$ at the i-th iteration, and it is defined as

$$\eta^{(i)} \triangleq \frac{\sum_{\tau} \sum_{m,n=1,m\neq n}^{M} |r_{mn}^{(i)}[\tau]|^2}{\sum_{\tau} \|\mathbf{R}[\tau]\|_{\mathrm{F}}^2}, \qquad (17)$$

where the notation $\|\cdot\|_{\mathrm{F}}$ denotes the Frobenius norm.

The comparison between these two PEVD algorithms is calculated via Monte Carlo simulations over an ensemble of 100 different random 10×10 para-Hermitian matrices of order 5, which can be generated from matrices $\underline{\mathbf{A}}(z) \in \underline{\mathbb{C}}^{10\times 10}$ of order 3 with i.i.d. zero mean unit variance complex Gaussian entries, such that $\underline{\mathbf{R}}(z) = \underline{\mathbf{A}}(z)\widetilde{\underline{\mathbf{A}}}(z)$. Fig. 3 shows the normalized off-diagonal energy $\eta^{(i)}$ versus the iteration index i. Obviously the MS-SBR2 algorithm requires much fewer iterations than the conventional SBR2 algorithm to achieve the same level of diagonalization. However, it should be noticed that each iteration within MS-SBR2 involves more rotation steps, which means the computational costs between them are comparable. Nonetheless, the MS-SBR2 algorithm was found to converge faster than SBR2 as shown in Fig. 4. For further details of the MS-SBR2 algorithm, see [13].

C. Accuracy of the Decomposition

There are two main factors which can affect the accuracy of the decomposition. Firstly, since the decomposition is performed upon the two para-Hermitian matrices $\underline{\mathbf{C}}(z)\widetilde{\underline{\mathbf{C}}}(z)$ and $\widetilde{\underline{\mathbf{C}}}(z)\underline{\mathbf{C}}(z)$ as shown in (5) and (6), the resulting diagonal matrix $\underline{\mathbf{\Sigma}}(z)$ might be less accurate than that found by the way of operating the decomposition directly upon the channel matrix $\underline{\mathbf{C}}(z)$. Secondly, in the sense of broadband MIMO decoupling, a strictly diagonalized channel matrix is required. However, the proposed PSVD method can only generate an approximately diagonal matrix subject to the pre-specified stop condition of the algorithm, so there will be errors when assuming all the off-diagonal elements of $\underline{\mathbf{\Sigma}}(z)$ are equal to zero. In addition, due to the fact that the orders of the polynomial matrices increase as the iteration goes throughout the PEVD process, the equalization becomes difficult when the order of $\underline{\mathbf{\Sigma}}(z)$ is too large. Therefore polynomial order truncation operations [20], [21] are usually required in order to keep orders as small as possible and reduce the computational cost of the algorithm, which can also cause a very small proportion of the total Frobenius norm of the matrix being eliminated. To assess how well the proposed PSVD method performs, the error metric of the PSVD is defined as

$$E \triangleq \frac{\left\| \underline{\mathbf{C}}(z) - \widetilde{\underline{\mathbf{U}}}(z)\widehat{\underline{\mathbf{\Sigma}}}(z)\underline{\mathbf{V}}(z) \right\|_{\mathrm{F}}^2}{\|\underline{\mathbf{C}}(z)\|_{\mathrm{F}}^2}, \qquad (18)$$

where $\widehat{\underline{\mathbf{\Sigma}}}(z)$ is equal to $\underline{\mathbf{\Sigma}}(z)$ with all the off-diagonal elements set to zero.

VI. Simulation Results

A. Example 1

To demonstrate the proposed PSVD method, a polynomial or broadband channel matrix $\underline{\mathbf{C}}_1(z) \in \underline{\mathbb{C}}^{4\times 3}$ was generated to describe the propagation of three source signals onto four sensors. Each of the polynomial entries of the matrix was chosen to be order-5 FIR filter, where both the real and imaginary parts were drawn randomly from a uniform distribution in the range $[-1, 1]$. A graphical representation of this channel matrix is plotted in Fig. 5. With the truncation and stopping parameters set as $\mu = 10^{-4}$ and $\epsilon = 10^{-3}$, the diagonalized channel matrix $\underline{\mathbf{\Sigma}}_1(z)$ from the PSVD by MS-SBR2 method is shown in Fig. 6, and the performance comparison against the PSVD by SBR2 method is summarized in Tab. I. The results presented in the table demonstrate that with the same level of decomposition achieved, i.e. $g = 9.91 \times 10^{-4}$, the PSVD by MS-SBR2 method outperforms the PSVD by SBR2 method in terms of the number of iterations, relative error and computational time.

In addition, akin to an ordered SVD with singular values in descending order, the power spectral densities (PSDs) $\underline{\sigma}_{mm}(e^{j\Omega}) = \underline{\sigma}_{mm}(z)|_{z=e^{j\Omega}}, m = 1, 2, \cdots, M$ of the diagonalized matrix $\underline{\mathbf{\Sigma}}_1(z)$ has the spectral majorisation property

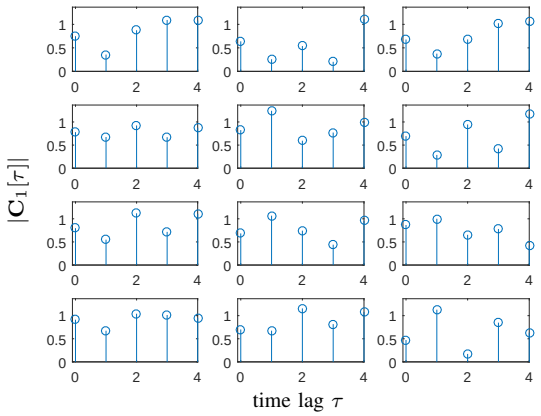


Fig. 5. The stem plot of the 4×3 broadband MIMO channel matrix $\underline{\mathbf{C}}_1(z)$ showing the magnitude of channel impulse response at different time lag.

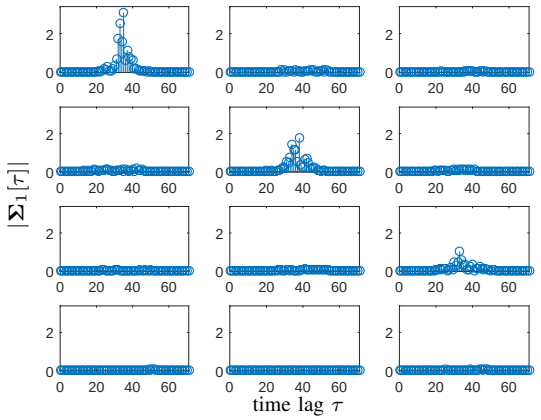


Fig. 6. The stem plot of the 4×3 diagonalized MIMO channel matrix $\underline{\mathbf{\Sigma}}_1(z)$ obtained using PSVD by MS-SBR2 method.

[22] such that for all normalised angular frequency values Ω

$$\underline{\sigma}_{11}(e^{j\Omega}) \geq \underline{\sigma}_{22}(e^{j\Omega}) \geq \cdots \geq \underline{\sigma}_{MM}(e^{j\Omega}). \qquad (19)$$

Compared to the original PSDs of $\underline{\mathbf{C}}_1(z)$ shown in Fig. 7, the PSDs of the diagonalized channel matrix $\underline{\mathbf{\Sigma}}_1(z)$ are spectrally majorised, which intuitively indicates that the MIMO channel has been decoupled into a set of independent SISO channels.

B. Example 2

This example shows the practical application of the MS-SBR2 algorithm to a measured (2×2) optical MIMO channel. In fiber-optic systems one method to realize a MIMO transmission is to carry the data streams on different optical modes through a few-mode or multi-mode fiber (MMF) [2],

TABLE I
RESULTS OF APPLYING THE PSVD BY PEVD ALGORITHMS TO $\underline{\mathbf{C}}_1(z)$ IN EXAMPLE 1

performance metrics	PSVD by	
	SBR2	MS-SBR2
converged value g	9.91×10^{-4}	9.91×10^{-4}
number of iterations	561	478
relative error E	0.0428	0.0377
computational time (sec.)	1.98	1.74

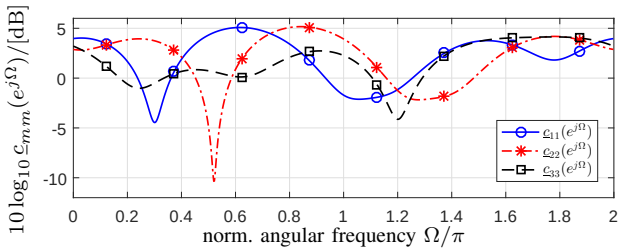


Fig. 7. The PSDs $\underline{c}_{mm}(e^{j\Omega}), m = 1, 2, 3$ of the channel matrix $\underline{\mathbf{C}}_1(z)$.

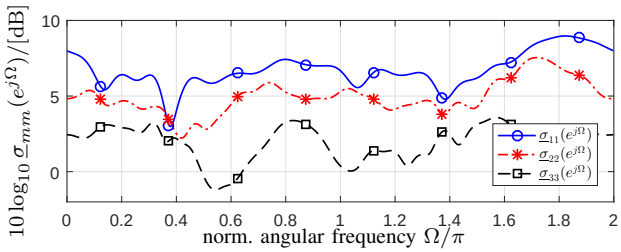


Fig. 8. The PSDs $\underline{\sigma}_{mm}(e^{j\Omega}), m = 1, 2, 3$ of the diagonalized channel matrix $\underline{\mathbf{\Sigma}}_1(z)$.

[23]. For the excitation of different modes, certain single-mode fiber (SMF) to MMF alignments with varying radial offsets δ are used in this work. The spatial diversity of the optical MIMO channel is visualized by showing the measured spatial intensity distributions when exciting the two optical MIMO inputs of the (2×2) system separately. The measured patterns depicted in Fig. 9 demonstrate that spatially diverse channels are generated. However, an ideal separation of the two channels is hard to achieve since mode mixing usually occurs in the mode multiplexing and demultiplexing process which is implemented by fusion couplers, and during the transmission through the fiber. An overview of the testbed used

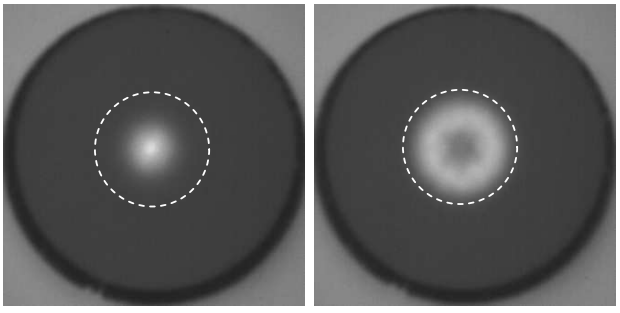


Fig. 9. Intensity distribution patterns at the end face of a MMF fiber when launching centric $\delta = 0$ µm (left) and launching with an eccentricity of $\delta = 15$ µm (right) measured at a wavelength of 850 nm; the dashed line represents the 50 µm core diameter.

for measuring optical MIMO impulse responses is shown in Fig. 10. Here the impulse responses of the (2×2) optical MIMO channel, consisting of a 1.4 km MMF, fusion couplers and differently aligned SMFs, are measured at an operating wavelength of 1576 nm with the aid of signal deconvolution [8]. The measured impulse responses are then sampled at the symbol rate of 620 MHz and used to constitute the channel matrix $\underline{\mathbf{C}}_2(z)$ as plotted in Fig. 11.

Applying PSVD to this frequency-selective MIMO channel

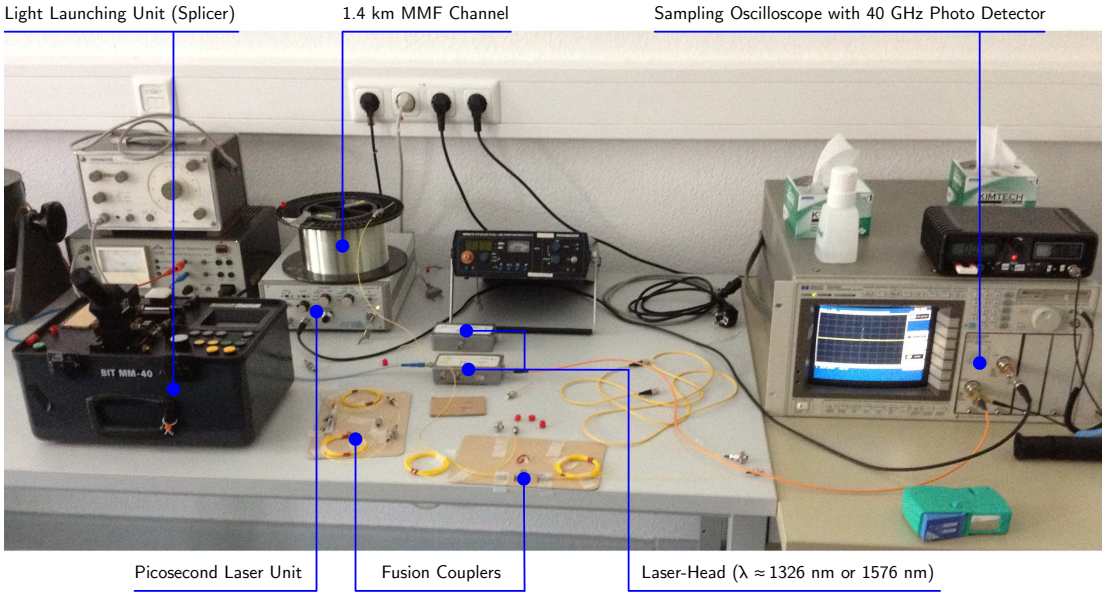


Fig. 10. Measurement setup for determining the MIMO specific impulse responses [25].

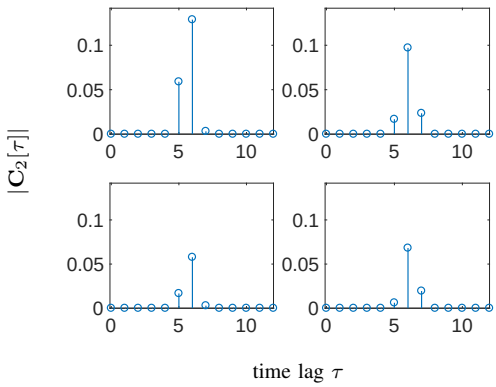


Fig. 11. The stem plot of the measured 2×2 optical MIMO channel matrix $\underline{\mathbf{C}}_2(z)$ showing the magnitude of channel impulse response at different time lag.

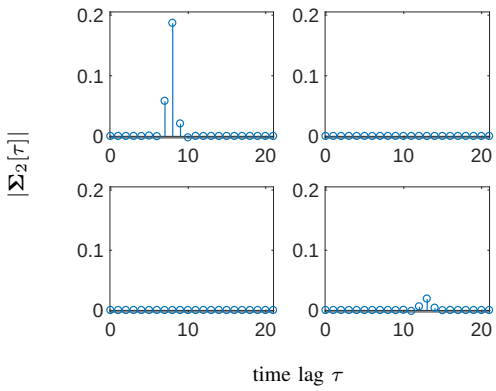


Fig. 12. The stem plot of the diagonalized 2×2 optical MIMO channel matrix $\underline{\mathbf{\Sigma}}_2(z)$.

results in layers having a time-dispersive characteristic and hence ISI occurs on each layer as shown by the diagonalized matrix $\underline{\mathbf{\Sigma}}_2(z)$ in Fig. 12. The remaining ISI is removed by applying the T-spaced zero forcing equalization as mentioned before. The equalizers modify the noise power on each layer differently, which is expressed by the weighting factors θ_ℓ, with ℓ denoting the layer index. These factors determine the layer specific SNRs and hence also the total BER performance [8]. In this example, the noise weighting factors for each layer are computed as $\theta_1 = 37.22$ and $\theta_2 = 4243.46$. In addition, the remaining off-diagonal energy ε, defined as $\varepsilon = \sum_\tau \|\mathbf{C}_2[\tau]\|_\mathrm{F}^2 - \sum_\tau \|\mathbf{\Sigma}_2[\tau]\|_\mathrm{F}^2$, is given by 1.26×10^{-6}. The value of ε is negligibly small compared with the input energy, which means that the CI has been significantly eliminated.

The BER quality is studied by using fixed transmission modes with a spectral efficiency of 8 bit/s/Hz, and the analyzed quadrature amplitude modulation (QAM) constellation arrangements are depicted in Tab. II. In addition to bit-loading,

TABLE II
TRANSMISSION MODES

throughput	layer 1	layer 2
8 bit/s/Hz	256	0
8 bit/s/Hz	64	4
8 bit/s/Hz	16	16

the allocation of the transmit power to the activated layers is needed to optimize the BER performance. In the optimum case, the PA aims at equalizing the BERs over all layers. However, this approach is computationally complex and hence it is simplified by just equalizing the SNRs as a sub-optimum solution. After the application of the T-PSVD, the decoupled MIMO layers exhibit decreasing SNRs at higher layers. This conforms with the spectral majorisation property shown in example 1. The SNR conditions subsequent to the PSVD

equalization and the conditions after power allocation are illustrated in Fig. 13.

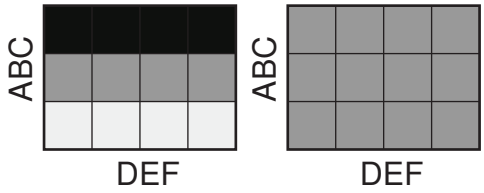


Fig. 13. Illustration of the remaining SNRs in T-PSVD systems without applying PA (left) and with PA (right). The color black refers to high and white to low SNR values.

The BER performance results for T-PSVD equalization, obtained by applying the MS-SBR2 algorithm for calculating the PSVD, are depicted in Fig. 14 for a range of SNRs. Here E_{s} is the transmit signal energy and N_0 denotes the constant noise power spectral density of the additive white Gaussian noise. As seen from the graph, the $(256, 0)$ QAM transmission scheme shows the best performance results. It should be noted that no PA is needed for the $(256, 0)$ QAM transmission mode. In addition, when activating multiple numbers of layers the benefit of using the equal SNR power allocation method is clearly visible. As the dimension of the polynomial matrices $\underline{\mathbf{C}}_2(z)\widetilde{\underline{\mathbf{C}}}_2(z)$ and $\widetilde{\underline{\mathbf{C}}}_2(z)\underline{\mathbf{C}}_2(z)$ is 2×2, this means that only one off-diagonal element can be eliminated for each iteration when computing the PEVD via the MS-SBR2 algorithm, i.e. $L^{(i)} = 1, \forall\, i$. Therefore, the MS-SBR2 algorithm operates the same as the SBR2 and there is no difference between them in terms of the BER performance for this example. However, in real world implementations involving more sources and sensors, the benefits of the MS-SBR2 algorithm could come into play.

It is expected that PSVD based MIMO systems can offer the same BER performance compared to systems based on STVC with SVD equalization, as it is suggested by the achievable spectral efficiencies presented in [24]. The major advantage of MIMO systems based on PSVD is that they do not require a block-wise transmission.

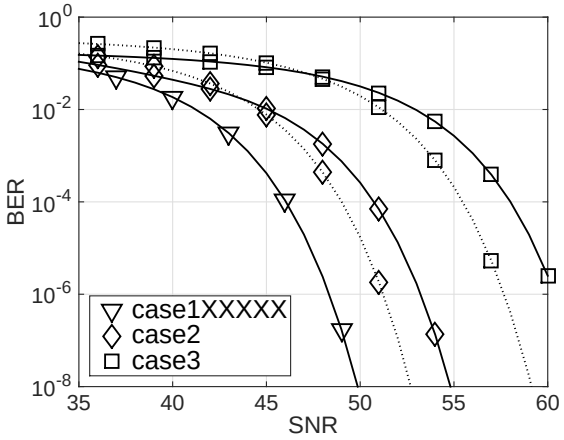


Fig. 14. BER with PA (dotted line) and without PA (solid line) by applying the T-PSVD equalization scheme, showing the comparisons among different transmission modes when transmitting over the 2×2 optical MIMO channel.

VII. Conclusion

We have investigated how the proposed MS-SBR2 algorithm can be used in the application of decomposing the channel matrix of a measured (2×2) broadband optical MIMO system. Furthermore, different transmission schemes have been employed to illustrate the BER simulations. In particular, the power allocation scheme has been utilized to further optimize the BER performance. Simulation results have shown that the activation of all transmission layers does not necessarily lead to the best BER performance. On the contrary, the $(256, 0)$ QAM with the T-PSVD equalization scheme seems to achieve the best performance in the studied example.

References

[1] A.C. Singer, N.R. Shanbhag, B. Hyeon-Min, "Electronic Dispersion Compensation – An Overview of Optical Communications Systems," *IEEE Signal Processing Magazine*, 25(6):110–130, 2008.

[2] P.J. Winzer, G.J. Foschini, "MIMO Capacities and Outage Probabilities in Spatially Multiplexed Optical Transport Systems," *Optics Express*, 19(17):16680–16696, 2011.

[3] G.C. Raleigh, J.M. Cioffi, "Spatio-temporal Coding for Wireless Communication," *IEEE Trans. Communications*, 46(3):357–366, Mar 1998.

[4] G.C. Raleigh, V.K. Jones, "Multivariate Modulation and Coding for Wireless Communication," *IEEE Journal on Selected Areas in Communications*, 17(5):851–866, Mar 1999.

[5] S.S. Haykin, *Adaptive Filter Theory*, 2nd ed., Upper Saddle River, NJ: Prentice-Hall, 1991.

[6] A. Scaglione, P. Stoica, S. Barbarossa, G.B. Giannakis, H. Sampath, "Optimal designs for space-time linear precoders and decoders," *IEEE Trans. SP*, 50(5):1051–1064, May 2002.

[7] C.H. Ta, S. Weiss, "A Design of Precoding and Equalisation for Broadband MIMO Systems," in *Asilomar Conf. Signals, Systems & Computers*, Pacific Grove, CA, pp. 1616–1620, Nov. 2007.

[8] A. Sandmann, A. Ahrens, S. Lochmann, "Resource Allocation in SVD-Assisted Optical MIMO Systems using Polynomial Matrix Factorization," *ITG-Fachtagung: Photonische Netze*, Leipzig, Germany, 2015.

[9] J.A. Foster, J.G. McWhirter, M.R. Davies, J.A. Chambers, "An Algorithm for Calculating the QR and Singular Value Decompositions of Polynomial Matrices," *IEEE Trans. SP*, 58(3):1263–1274, Mar. 2010.

[10] J.G. McWhirter, "An Algorithm for Polynomial Matrix SVD Based on Generalised Kogbetliantz Transformations," in *18th EUSIPCO*, pp. 457–461, Aalborg, Denmark, Aug. 2010.

[11] J.G. McWhirter, P.D. Baxter, "A Novel Technique for Broadband Singular Value Decomposition," in *12th Annual ASAP Workshop*, MA, USA, Mar. 2004.

[12] J.G. McWhirter, P.D. Baxter, T. Cooper, S. Redif, J. Foster, "An EVD Algorithm for Para-Hermitian Polynomial Matrices," *IEEE Trans. SP*, 55(5):2158–2169, May 2007.

[13] Z. Wang, J.G. McWhirter, J. Corr, S. Weiss, "Multiple Shift Second Order Sequential Best Rotation Algorithm for Polynomial Matrix EVD," in *23rd EUSIPCO*, pp. 844–848, Nice, France, Aug. 2015.

[14] A. Tarighat, R.C.J. Hsu, A. Shah, A.H. Sayed, B. Jalali, "Fundamentals and challenges of optical multiple-input multiple-output multimode fiber links," *IEEE Communications Magazine*, 45(5):57–63, May 2007.

[15] P.P. Vaidyanathan, *Multirate Systems and Filter Banks*, Prentice-Hall, 1993.

[16] S. Icart, P. Comon, "Some properties of Laurent polynomial matrices," in *IMA Conference on Mathematics in Signal Processing*, Birmingham, UK, Dec. 2012.

[17] S. Redif, S. Weiss, J.G. McWhirter, "Sequential Matrix Diagonalization Algorithms for Polynomial EVD of Parahermitian Matrices," *IEEE Trans. SP*, 63(1):81–89, Jan. 2015.

[18] J. Corr, K. Thompson, S. Weiss, J.G. McWhirter, S. Redif, I.K. Proudler, "Multiple Shift Maximum Element Sequential Matrix Diagonalisation for Parahermitian Matrices," in *IEEE SSP Workshop*, pp. 312–315, Gold Coast, Australia, Jun. 2014.

[19] Z. Wang, J.G. McWhirter, J. Corr, S. Weiss, "Order-controlled multiple shift SBR2 algorithm for para-Hermitian polynomial matrices," in *IEEE SAM Workshop*, pp. 1–5, Rio de Janerio, Brazil, Jul. 2016.

[20] J. Foster, J.G. McWhirter, J. Chambers, "Limiting the Order of Polynomial Matrices Within the SBR2 Algorithm," in *IMA Conference on Mathematics in Signal Processing*, Cirencester, UK, Dec. 2006.

[21] C.H. Ta, S. Weiss, "Shortening the Order of Paraunitary Matrices in SBR2 Algorithm," in *Int. Conference on Information, Communications & Signal Processing*, pp. 1–5, Singapore, Dec. 2007.

[22] P.P. Vaidyanathan, "Theory of optimal orthonormal subband coders," *IEEE Trans. SP*, 46(6):1528–1543, Jun 1998.

[23] A. Sandmann, A. Ahrens, S. Lochmann, "Experimental Description of Multimode MIMO Channels utilizing Optical Couplers," *ITG-Fachbericht 248, Photonische Netze*, pp. 125-130, 2014.

[24] A. Sandmann, A. Ahrens, S. Lochmann, "Performance Analysis of Polynomial Matrix SVD-based Broadband MIMO Systems," *Sensor Signal Processing for Defence Conference (SSPD)*, pp. 50–54, 2015.

[25] A. Sandmann, A. Ahrens, S. Lochmann, "Zero-Forcing Equalisation of Measured Optical Multimode MIMO Channels," *Communications in Computer and Information Science (CCIS 554), Springer International Publishing*, 2015.

Zeliang Wang received the B.Eng. degree in communications engineering from Northwest University for Nationalities, Lanzhou, China, in 2011 and the M.Sc. degree (distinction) in communications engineering from the University of York, York, U.K., in 2012. He is currently working toward the Ph.D. degree in the Centre of Digital Signal Processing, School of Engineering, Cardiff University, Cardiff, U.K., under the supervision of Prof. J. G. McWhirter. His research interests are in polynomial matrix techniques, sensor array processing, blind signal separation and MIMO communications.

André Sandmann received the B.Eng. and M.Eng. degree in information and electrical engineering from the Hochschule Wismar, University of Applied Sciences: Technology, Business and Design, Germany, in 2014 and 2016, respectively. Currently he is research scientist at the Communications Signal Processing Group, Hochschule Wismar. His research interests include MIMO communications systems, fiber-optic communication and signal processing.

John G. McWhirter received the B.Sc. degree (first class honors) in mathematics and the Ph.D. degree in theoretical physics from the Queens University of Belfast, Belfast, Ireland, in 1970 and 1973, respectively. He joined the Royal Radar Establishment in Malvern (later to become the Royal Signals and Radar Establishment, and now part of QinetiQ Ltd.) in 1973, where he became a Senior Fellow in the Centre for Signal and Information Processing Group. In 2007, he left QinetiQ to take up his current post as Distinguished Research Professor at the School of Engineering, Cardiff University, Cardiff, U.K. He is also a Visiting Professor in Electrical Engineering at the Queens University of Belfast. He has been carrying out research on adaptive signal processing since 1980. He has published more than 140 research papers and holds numerous patents. His current research is devoted to broadband sensor arrays, convolutive blind signal separation, and polynomial matrix techniques.

Dr. McWhirter was elected as a Fellow of the Royal Academy of Engineering in 1996 and as a Fellow of the Royal Society in 1999. He is a Fellow of the Institute of Mathematics and its Applications (IMA) and served as President of the IMA in 2002 and 2003. He is also a Fellow of the Institute of Electrical Engineers, a Fellow of the Institute of Physics, and a member of the London Mathematical Society. The signal processing group which he built up in Malvern over many years, received the EURASIP Group Technical Achievement Award for 2003. He was awarded the J. J. Thomson Medal by the Institution of Electrical Engineers in 1994 for his research on systolic arrays.

Andreas Ahrens received the Dipl.-Ing. degree in electrical engineering from the University of Rostock in 1996. From 1996 to 2008, he was with the Institute of Communications Engineering of the University of Rostock, from which he received the Dr.-Ing. and Dr.- Ing. habilitas degree in 2000 and 2003, respectively. In 2008, he became a Professor for Signal and System theory at the Hochschule Wismar, University of Technology, Business and Design, Germany. His main field of interest includes error correcting codes, multiple-input multiple-output systems and iterative detection for both wireline and wireless communication.

Botnet C&C Traffic and Flow Lifespans Using Survival Analysis

Vaclav Oujezsky, Tomas Horvath and Vladislav Skorpil

***Abstract*—This paper addresses the issue of detecting unwanted traffic in data networks, namely the detection of botnet networks. In this paper, we focused on a time behavioral analysis, more specifically said – lifespans of a simulated botnet network traffic, collected and discovered from NetFlow messages, and also of real botnet communication of a malware.**

As a method we chose survival analysis and for rigorous testing of differences Mantel–Cox test. Lifespans of those referred traffics are discovered and calculated by lifelines using Python language.

Based on our research we have figured out a possibility to distinguish the individual lifespans of C&C communications that are identical to each other by using survival projection curves, although it occurred in a different time course.

***Keywords*—Botnet, Lifespans, Modeling, NetFlow, Survival Analysis,**

I. Introduction to the Problem

Nowadays, rapid networks demand developing of sophisticated method to uncover an unusual behavior of network traffic. Progressively, new techniques are being developed to predict or detect network behavior. These techniques collect traffic information from devices as Test Access Point (TAP), they use port mirroring techniques or they perform an analysis of NetFlow messages [1].

Our statistics survey shows that the most analysis approach of network anomalies detection is based on ”store and backmine” data to analyze it from a database or systems use regular expressions. Anomalies can be marked as intentional and unintentional. Intentional could be botnet networks, distributed denial of services (DDoS) attacks etc. Unintentional anomalies are errors in networks, for example.

This is an extended paper, previously published by International Conference on Telecommunications and Signal Processing (TSP) [2], and the intention of our research is to define and expand a method how to analyze malevolent communication among clients and servers which communicate over a wide transport network. The certain groups of devices can play a basic role in botnet. The word botnet is a combination of the words robot and network. It is very difficult and complex issue. More types of botnet networks and their behavior are distinguished [3]. The basic is with Internet Relay Chat (IRC) communication approach. The another types of botnet are: with the Hypertext Transfer Protocol (HTTP), Point to Point (P2P) and HTTP2P traffic combined, centralized and decentralized.

There are several types of traffic types than described above. Generally, a botnet network can be controlled and commanded with any type of access to the root privileges of devices. Such access can be deployed by Secure Shell (SSH) connectivity or, as is an different example, with e–mail access. Such technique is also used in the project GCAT [4], it uses a gmail account to create Command and Control (C&C) channels.

C&C channels represent receiving and sending commands and informations between botmaster (C&C server) and infected clients (C&C clients), as is shown in Fig. 1. Botmaster can affect and control many clients in short time period. With this control, clients can do a wholesale attack.

Given the above, we distinguish many types of existing approaches and methods how to create a botnet. What is essential to say that the process of taking control of network devices is not firmly defined and can be done basically by any individual approach, also by creating a custom solution and this solution would be for others unknown and unpredictable.

The detection of botnet is generally based on methodology behavior or signature and C&C infrastructure. Since a communication in botnet also demands to carry information, it can be utilized for the detection. The main issue is, that this communication or traffic is mixed with others. Then, the behavior of this malicious traffic can be similar as a normal traffic. If an intrusion detection system is used for the detection, there is again problem with the traffic encryption used between C&C machines and rule signatures cannot be applied.

From our previous research, our decision and goal is to

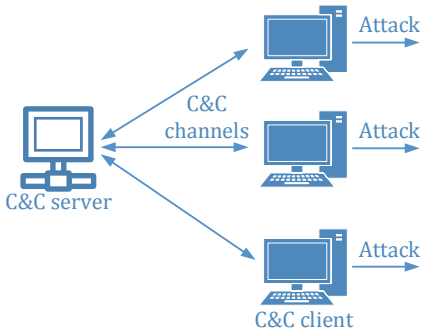


Fig. 1. Simple centralized botnet network

Manuscript received October 26, 2017, revised March 8, 2017.

Research described in this paper was financed by the National Sustainability Program under grant LO1401. For the research, infrastructure of the SIX Center was used.

V. Oujezsky, T. Horvath and V. Skorpil are with the Faculty of Electrical Engineering and Communication Brno University of Technology, Technicka 3058/10, BRNO 616 00 CZ. Corresponding author to provide (e-mail: vaclav.oujezsky@phd.feec.vutbr.cz).

survey the possibilities of detection these networks based on graph theory and time's persistence. What is very important, it is not sure if the botnet behavior is ergodic, stationary normalized or both or not. The final proof of it do not still exists regards to our discussion on teleconferences with other professionals. The focus has to be also on its stochastic.

The rest of this paper is structured as follows. The next section II presents a description of the related works. After section III, the basic methods, techniques and principles used are explained. The following section describes the methods of testing and the results, then the discussion within a conclusion is presented.

II. Related Work

Until now, there have been several approaches used for the detection of botnet or malicious traffic. These approaches can be divided into the following categories, from the viewpoint of focus:

- Host-based detection.
- Network-level-based detection.
- Graph-Theory-based detection.

We are generally concerned in Network–level and Graph–Theory combined based detection. In both, numerous works have been addressed to these topics.

Host-based detection mixed with the Network-level based was chosen in paper [5], where the authors performed Behavioral Classification. Sérgio S.C. Silva et al. presented in [3] a comprehensive view on the issue of botnet networks. We take over principles of botnet behavior. Graph theory and cyber–thread infrastructure is covered by an article [6]. The authors also present "badness scores for domains", IP addresses. It leads us to the idea to do the comparative score for our NetFlow duration.

The Network-level-based approach has been presented in [7], where the authors used flow data collected from a backbone network to detect e-mail spammers. The similarity with our work is in how we gathered data to our analysis from a backbone devices.

Detailed research in this topic is presented by Stebastián García et al. The authors are interested in Botnet C&C Behaviors. Their work is concerned in the time-based behavioral characteristics. In article [8] the identification of the User Datagram Protocol (UDP), Transmission Control Protocol (TCP) and HTTP C&C channels and its analysis is presented. The second article [9], from which we were inspired, provides a comprehensive view of the comparison of the ways and possibilities to botnet detection. We adapted the method of "Aggregate the NetFlows by source Internet Protocol (IP) address" and the motivation to do the aggregation of NetFlow. Here are the properties of botnet (citation):

- Each bot communicates with the C&C server periodically.
- Several bots may communicate at the same time with the same C&C servers.
- Several bots attack at the same time the same target.

Our different approach is in the NetFlow aggregation and in the method of post-processing. From this research it is obvious that the communication among clients and servers has a certain periodicity and they communicate with a readable frequencies. A closer look at all the approaches currently used, due to the nature of the botnet network, it seems perspective to continue to deal with the combined model behavior and data collection.

To sum it up, many articles have been written about botnet and behavior. Not much has been written about the life-cycle of the botnet. The main question for us is given: what is the average lifespans of botnet, what about life-cycle? How to determine it with using existing network devices in a converged transport network.

III. Methods, Techniques and Principles Used

A. NetFlow and its use

NetFlow has been involved and implemented by company Cisco Systems, Inc in their network products [10]. This method is very popular and widely deployed by manufacturers of network elements of different brands. Latest successor of it is Internet Protocol Flow Information Export (IPFIX). These messages are used to send information about passing traffic from network devices to an analyzer (collector).

An example is Scrutinizer [1] – used for aggregating NetFlow protocol messages sent from individual network devices. If the network devices are configured appropriately, they periodically send NetFlow protocol informations about which nodes (IP addresses) communicate. It sends information about TCP and UDP ports and also information about the duration of a connection. If the information about entire network are aggregated in one place, than can be fairly accurately identified certain types of attacks against the network typically volumetric DoS / DDoS attacks, attempts to SYN flooding etc. It can also identify certain types of attempts of illegal penetration into the network and other incidents. This all depends on the quality of the collector, its ability statistical processing of individual NetFlow reporting.

Another use of NetFlow is a collection of "traffic data" named Data Retention (DR), which requires not only the Czech legislation. In the Czech Republic (CR), it is a law of "electronic communications" (no. 127/2005), specifically 97 paragraph 3. This law was based originally on a directive of the European Parliament and Council Directive 2006/24/EC. This directive was invalidated in 2013. It is therefore likely that a substantial number of European Union countries have legislation which is similar in intent to this CR law. The essence of the use of NetFlow within the DR is storing NetFlow reports and export them to the legitimate applicants in the original – unchanged – form.

NetFlow is also used by administrators of large corporate networks. It is primarily for monitoring of which node (computer / server) is communicating at a given time.

For daily use, the most important are algorithms, which are decisive. It is important that the collector only reports real

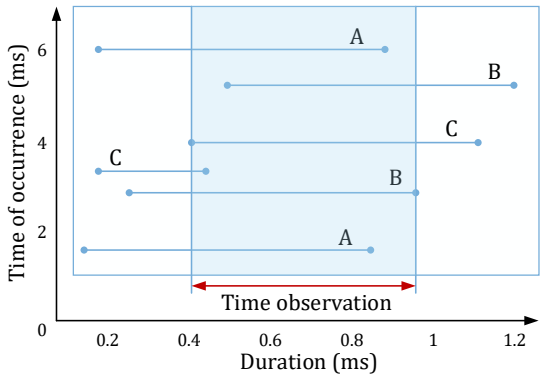


Fig. 2. Time of observed epoch

attacks and does not generate the number of false positives reactions.

B. Survival Analysis

Survival analysis was originally developed to measure lifespans of individuals. This analysis can be applied to any process duration. For example, it can be related to a web service, where the start of duration users are joining and the end is when the users leave the web service. Survival function is defined as:

$$S(t) = Pr(T > t) \tag{1}$$

where T represents random lifetime taken from a set of population and function $S(t)$ is defined as the probability of surviving until at least time t [11], equivalently, it defines the probability, that the death event of subject has not occurred yet at time t.

Survival function with the statement above has following properties, $0 \leq S(t) \leq 1$, $F_T(t) = 1 - S(t)$, where $F_T(t)$ is the CDF of T and $S(t)$ is non increasing function of t.

1) Censoring and truncation: Further, right and left censorship is defined. With the right-censored individuals we have information only about their current lifelines duration. On the other hand, with the left-censored individuals we do not know information about their birth (formation, start). The last type of censoring is the interval-censored. In this case we do not know exact time without event. We have partially observed events. The truncation happens, when the subjects have been at even before entering the study. Survival analysis is a very useful tool to understand duration.

Fig. 2 represents our example case of study with different combination of events and their start and end, thus duration. Letter *A* is a normal traffic, letter *B* and *C* would be C&C communications. Our aim is to find out the shape and result of survival function of each traffic for a protocol, port or IP address and compare them with one another. In our case, two survival functions of C&C traffic should be "almost" similar, even if they take place in a different time sequence, with regard to the conditions specified in [9] we set up behavior of botnet.

For the indication of the length of observation the random variable *T* is used. It expresses all captured NetFlows. δ is an indicator of the event. In case an event has occurred, δ is equal to 1 and if the individual was censored δ is equal to 0. For n studied subjects a plurality of pairs $\{(t_i, \delta_i), i = 1 \ldots n\}$ is received.

2) Estimating the Survival function: Kaplan–Meier estimator has been used within our test to estimate the survival function. It is a non–parametric method, therefore it does not require knowledge of the probability distribution that governs the survival of individual subjects. It is also called the product–limit method [11], [14]. Kaplan–Meier method gives an estimate of the survival function at every moment, in which there was a monitored event. The Kaplan–Meier Estimate is defined as:

$$\hat{S}(t) = \prod_{t_i < t} \frac{n_i - d_i}{n_i} \tag{2}$$

where d_i are the death events at time t_i and n_i are subjects at risk of death just prior to time t_i.

3) Compliance tests: Compliance tests of survival functions are used to compare two survival curves. There are many types of these tests, each of them has optimal properties for different situations. We could mention the Breslow test or the Tarone–Ware test. The most famous asymptotically valid tests include non–parametric Mantel–Cox test, named after Nathan Mantel and David Cox. Sometimes it is also named as "log rank test". The censoring process is independent here of the process that leads to the event. Mantel–Cox Chi–Squared is defined [14]:

$$\chi^2_{MC} = \frac{(O_1 - E_1)^2}{E_1} + \frac{(O_2 - E_2)^2}{E_2} \tag{3}$$

where the O_1 is the sum of occurrence of events for experimental group and the O_2 is the sum of occurrence of events for control group. The E means expected sum for each group.

Mantel–Cox test is also generalized to test more than two test's groups. Then, the equation 3 is just extended by $k - 1$ definitions $\chi^2_{MC} = k_1 + k_2 + k_n$. We compared with this test each traffic event and we observed its conformity, if two or more flows are similar or not.

C. Principle of use

From the base of botnet communication, it is very difficult to identify C&C traffic in transport network, where it is not possible to do a deep packet analysis. At first, it is not allowed by law, and the second reason, it is not effective to observe each packet and it is also time consuming. The situation is as difficult as decentralized this communication is. Therefore, we have focused on the traffic behavioral to find some stochastic in it.

We could effectively use existing devices on borders in a large transport network to send flow messages to a database collector and analyze timestamps, UNIX time and type of ports of regarded traffic. The idea is that we compare each time duration of a traffic given in UNIX time and we are looking for lifespans of it. After it, it is possible to compare survival curves with the log rank test. Because C&C messages have to be send at once by server to do an attack, we can observe and

find time reciprocity in a network to estimate that it is non demanded traffic.

D. Test's environment

Fig. 3 shows an involvement of component in the laboratory. We developed GDP-1.0.0 NetFlow collector (GDP) [12], which is an application in Python language used to collect NetFlow messages of version 1 and 5.

For the modeling traffic lifespans we have used NetFlow messages of version 5. This application has a database (sqlite3 database file) and collects information from NetFlow messages as is: source IP address, destination IP address, source port, destination port, protocol number, timestamps, first time, last time and system up-time. This application runs on virtual Windows 10 and is developed for Python version 3.

Two Cisco routers were configured and used to send NetFlow messages version 5 to the GDP application. Both of them have different subnet assigned and the passing traffic is mixed with laboratory traffic.

We followed the idea to create own C&C server and we have programmed Python code on different virtual PC as the C&C server. C&C channel feature SSH connectivity to C&C clients. The command channels are provided using the `fabric` module [13], [15] of Python. Finally, the algorithm used periodically connects and sends demands toward clients.

In this case, we simulated a periodic operation of the server and the clients regardless of the type of traffic. In real traffic also a certain frequency of C&C occurs and is primarily the possibility to detect a relationship between these frequencies, whether they appear at any time, and different subnet.

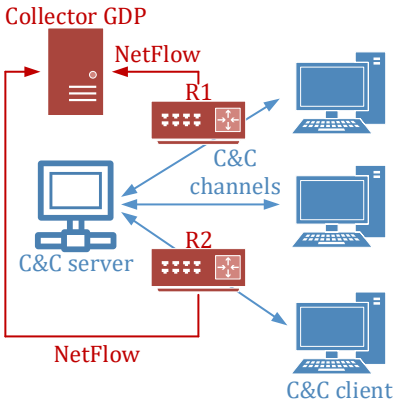


Fig. 3. Involvement of components in the laboratory

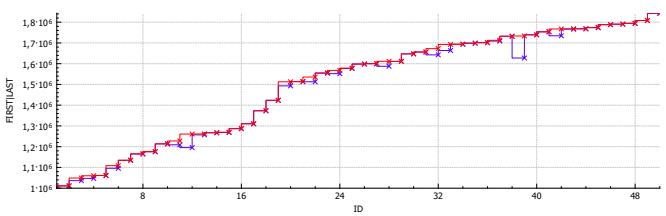


Fig. 4. FIRST/LAST time graph of captured flows I.

IV. Testing and Results

We observed similar duration and frequency in mixed traffic. Lifelines module [16] of Python as a implementation of survival analysis has been used for this purpose. It offers all of basic principles used in Survival Analysis. One limitation is with the other types of censorship. Interval-censored censorship is not implemented in lifelines yet. But the right-censored, left-censored and left-truncated censorship are included.

A. Initial Functional Test

At the beginning of the test, we examined the functionality of the program and the possibility of selection of network traffic and to display the lifelines.

We have compiled a test network over the public Internet using μtorrent clients. One of these clients was a server (sender) and the second was a receiver. Repeatedly, in a different timespan we transferred a reference file with the size of 100 MB.

These data were headed and a data–frame with the traffic information has been created and extracted in format as shown partly below:

	IP_SOURCE	IP_DEST	t	delta
0	192.168.1.11	192.168.1.1	7993	1
1	192.168.1.46	192.168.1.255	1	1
2	185.76.11.73	192.168.1.66	957	1
3	192.168.1.11	192.168.1.1	8089	1
4	192.168.1.11	192.168.1.1	7989	1
5	192.168.1.66	93.153.104.0	161721	1
6	192.168.1.46	192.168.1.11	161721	1
7	192.168.1.11	192.168.1.46	161741	1

The first three columns show IP source, IP destination and the t which is the duration of communication, taken from the value UNIX time of NetFlow. This value is calculated from `SysUptime` at the time the last packet of the flow was received minus `SysUptime` at start of flow. The fourth column shows a value $delta$. It represents the censorship. The value of the $delta$ is 1 due to the communication which ended during the reference period. In this case, all of the traffic has been terminated in the selected window time.

The graphs, plotted in Fig. 4 and 5 show all captured flows (ID) and the last time (red line) and the first time (blue line) of the two transmissions of the 100 MB reference file. It also includes the normal traffic. As seen, in this type of graph representation it is not possible to find any dependencies. Also, the amount of captured flows is not the same.

Furthermore, we separated the communication of the μtorrent's server and client. In this test case, we know the

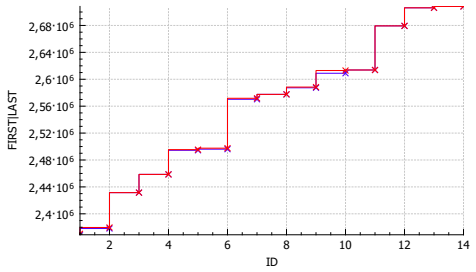


Fig. 5. FIRST/LAST time graph of captured flows II.

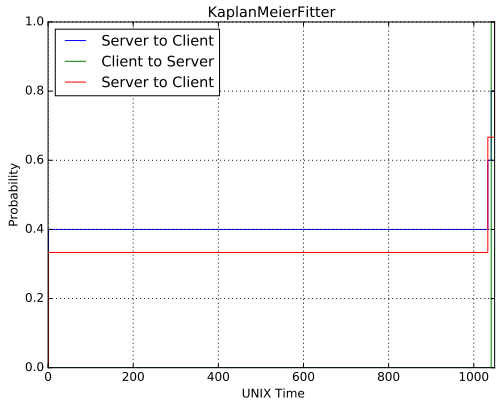


Fig. 6. Survival curve

IP addresses of these devices. This communication has undergone an analysis of Kaplan–Meier estimator with the left-censorship. The result is shown in Fig. 6. The curves of server–client communication in dependence on time and the probability is approaching to close identity even if they were taken at different time period.

This result was subjected to log rank test. This test is used to test the null hypothesis that there is no difference between the probability of an event at any time point.

Each group of server–client communication has been taken in different time scope. In group 1 the proper IP address was 5 times observed and in the group 2 the proper IP address was observed 3 times. So, the score is 5:3. The following listing is an extract from the log rank test performed:

```
Results
null distribution: chi squared
df: 1
t 0: -1
test: logrank
alpha: 0.05

_p-value|test statistic|_test result _|is significant
0.80408 |        0.062 |  Reject Null |        True
```

A p-value of less than 0.05 based on the log rank test indicates a difference between the two survival curves. In our case it is the value of $\cong 0.8$, which represents a value close to the maximum consensus of the two survival curves of server–client communication. The p-value of normal traffic comparing

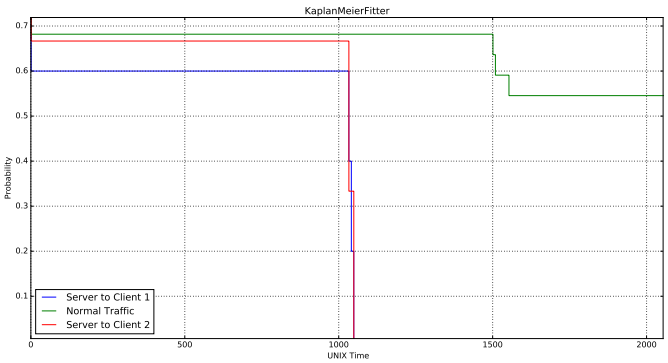


Fig. 7. KM estimate right censored - dependence test

server–clients traffic was 0.00735.

The initial functional test was successful and we obtained the values and survival curves for tested communication. The next provided test was a dependence test of C&C channels.

B. C&C Dependence Test

The test of C&C channels was assembled as is described above. C&C server periodically followed up SSH communication to the C&C clients placed in different subnetworks. This communication had been mixed by normal traffic. Captured communication using NetFlow reporting was again transferred to the Python `panda` data–frame by the GDP application.

In Fig. 7 the mutual comparison of survival's curves can be seen. The red line and the blue line are curves of C&C communication and the green line expresses the plot of normal traffic. The shortened example of format of event table obtained is following:

```
The duration of KM 1 is [1049 1041    1 1033    1]
          removed  observed  censored  entrance  at_risk
event_at
0               0         0         0         5        5
1               2         2         0         0        5
1033            1         1         0         0        3
1041            1         1         0         0        2
1049            1         1         0         0        1
```

We form the table in a modified form. This disposition of the table presents how many events were obtained for each duration. And the duration creates event time. The p-value, compare normal laboratory traffic and simulated C&C traffic was 0.17090 in comparison with the p-value of both of C&C was $\cong 0.75$. Again, we were able to find and to distinguish each communication channel.

V. Real Botnet Observation with Lifelines

We continued to observe data from real botnet network communication and apply proposed analysis to create its lifespans model. The .csv file of CTU-Malware-Capture-Botnet-1 [17] has been used as background information. The information of infected machine: Windows Name: Win8, IP: 10.0.2.22 (Label: Botnet-V1). All detailed information are given on author's website.

Database file "dataset" has been created by importing .csv file into it. For this testing purpose, we limited the number of inputs to 1,000,000. We isolated the communication of the machine x.22 and separately, we conquered the traffic to KaplanMeierFitter with the left censorship. The data have been headed and dataframe with traffic information created and extracted in the format as is shown partly below.

```
0                    SrcAddr           DstAddr         T C
1         00:00:00:00:00:00 00:00:00:00:00:00  0.000000 0
2                  0.0.0.0         10.0.2.22  2.003218 1
3                       :: ff02::1:ff01:e8a5  0.000000 0
4  fe80::705a:530f:1701:e8a5          ff02::2  4.003125 1
5  fe80::705a:530f:1701:e8a5         ff02::16  0.498083 1
6  fe80::705a:530f:1701:e8a5          ff02::2  0.000000 0
7  fe80::705a:530f:1701:e8a5        ff02::1:2  3.004039 1
8                 10.0.2.22          10.0.2.2  0.000096 1
...                     ...               ...       ... .
999970            10.0.2.22          8.8.8.8  0.010117 1
999971            10.0.2.22          8.8.8.8  0.010097 1
999972            10.0.2.22     94.100.176.20  0.000927 1
999973            10.0.2.22     74.125.142.26  0.001110 1
```

A. *Analysis of botnet traffic*

Once this set was formed, was subjected to analysis, see Fig. 8. Generally, the y-axis represents the probability communication is still around after the X time. In this case, the lifelines were observed for a particular service of the botnet as TCP, UDP, SPAM, Domain Name Service (DNS), and for background communication as well. The outputs are in one figure to make them easy read and comparability. It creates together their event table. Then, the median values, duration, and confidence intervals were calculated as is shown below.

```
The median of background is 0.000436
The median of background_arp is 1.898133
The median of botnet_1_UDP_Attempt is 2.193814
The median of botnet_1_TCP_Attempt is 3.003442
The median of botnet_1_TCP_Established is 0.353073
The median of botnet_1_UDP_Established] is 0.180717
The median of botnet_1_SPAM is 0.00136
The median of botnet_1_DNS is 0.010147
```

So far, we have formulated values for Win8. At the time-axis can, therefore, be selected certain time, for which we have defined probability. We assume, that this probability should be comparable independently of an occurrence. Now, we are able to compare background traffic with the each separate service of botnet traffic or whole botnet communication with the background traffic and observe the p-values and significance.

We have used the separate instance of Kaplan-Meier fitter to observe the difference between the botnet traffic and the background traffic and, it has been associated with one subplot, as shown in the Fig. 9. The result is significantly different only in the time line.

The same values we subjected the log rank test. The value p-value was less than the set limits, p-value < 0.000. The value of the test statistic was 249,388. Again, we have used chi squared null distribution and alpha 0.5.

We are also interested in the probability of distribution of represented protocols. The following Fig. 10 shows the difference in this probability after time n. The y-axis represents the probability a protocol is still around after t timeline, where t ms is on the x-axis. We also see that the shaded area of confidence interval is different for each protocol. The

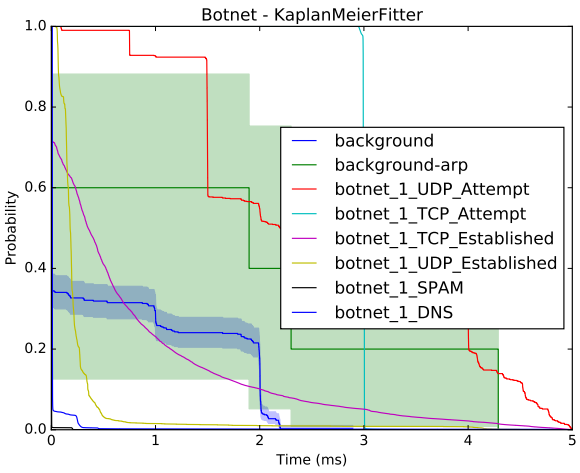


Fig. 8. KM estimate of Botnet of source 10.0.2.22

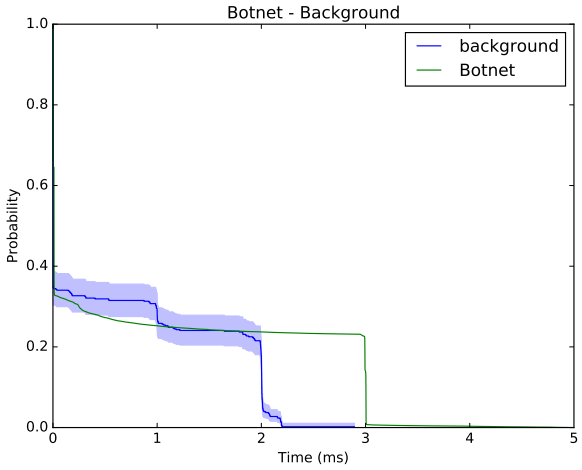


Fig. 9. Comparation of KM estimate of botnet and background traffic

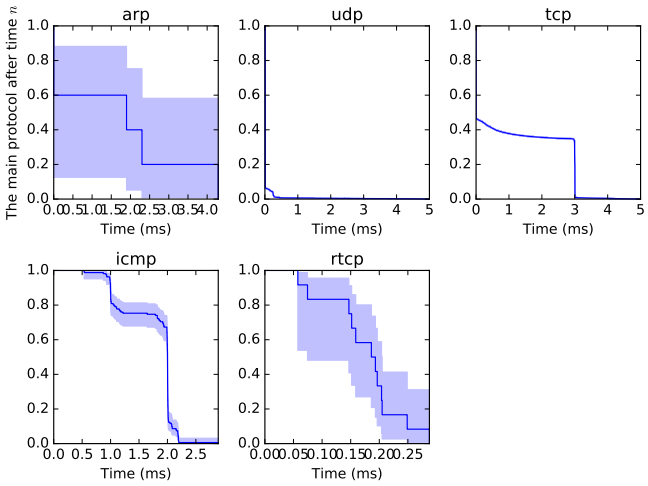


Fig. 10. KM estimation of protocols

confidence interval is the effect of sample size, methods of selection and population size, and it for the survival curve, whose reliability reaches values of $100(1-\alpha)$ for a given time t. From this point of view we have a reference map of the traffic.

VI. Concluding Remarks

The numerous methods are developed to detect botnet and others malicious traffic in heterogeneous networks. In this paper, we present a method for detecting command and control channels of a botnet. Our method is based on behavioral analysis and includes unique combination of the features as is the flow collector combined with survival analysis method. We created own application to simulate this C&C channel and also GDP-1.0.0 application to collect and store NetFlow messages.

We subtracted information form NetFlow messages, such as: duration of each communication in UNIX time, IP addresses and ports. We then created data–frames from this obtained information and we have subjected them to the survival analysis. This processing of NetFlow has shown the possibility of

detection of two traffic that are time-independent themselves, so the results demonstrate the possibility of detection by this method based on the time-duration.

By defining method above, we have used the .csv file of CTU-Malware-Capture-Botnet-1 to create a sample model of lifespan. The individual values and appearance of the function of lifespan were counted. These values are stored for future use as a pattern.

The benefit of this method is that it does not need to have a knowledge about proper time when a traffic occurs. It only needs to have knowledge about the duration of flows. Similarly, as in the case of traffic modeling using Markov chain, the appearance of communication is modeled. But with the difference, that traffic patterns are not generated, but two or more similar progressions are sought according to the previous conditions of behavior of botnet networks. This method accelerates a selection which traffic choose to the shortlist to decide whether the traffic is demanded or not.

In future work, we would like to extend our work to observe the survival values of Win12 of CTU-Malware-Capture-Botnet-1 and calculate multivariate log rank test. We would like to continue calculating values for each dataset. We plan to build own laboratory environment for capturing botnet communication and its evaluation method described above.

REFERENCES

[1] Plixer: *Flow Analytics*. PLIXER INTERNATIONAL, Inc. Plixer-Malware Incident Response.

[2] V. Oujezsky, T. Horvath and V. Skorpil, "Modeling Botnet C& C Traffic Lifespans from NetFlow Using Survival Analysis," in *Proc. 39th International Conference on Telecommunication and Signal Processing, TSP 2016*. Vienna, Austria 2016. pp. 50–55, ISBN 9781509012879, ISSN 1805-5435.

[3] S.C.S. Silva, R.M.P. Silva, R.C.G. Pinto, and R.M. Salles, "Botnets: A survey," *Computer Networks*, vol. 57, pp. 378–403, February 2013.

[4] GCAT: A fully featured backdoor that uses Gmail as a C&C server, GitHub.

[5] J. McHugh, R. McLeod, and V. Nagaonkar, "Passive network forensics: behavioural classification of network hosts based on connection patterns," *ACM SIGOPS Operating Systems Review*, vol. 42, pp. 99–111, April 2008.

[6] A. Boukhtouta, D. Mouheb, M. Debbabi, O. Alfandi, F. Iqbal, and M.E. Barachi, "Graph-theoretic characterization of cyber-threat infrastructures," *Digital Forensics & Incident Response*, vol. 14, pp. S3–S15, August 2015.

[7] W.K. Ehrlich, A. Karasaridis, D. Liu, and D. Hoeflin, "Detection of spam hosts and spam bots using network flow traffic modeling," in *Proc. 3rd USENIX conference on Large-scale exploits and emergent threats LEET'10*, pp. 7-7, ©2010.

[8] S. Garcia, V. Uhlir, and M. Rehak, "Identifying and modeling botnet C&C behaviors," in *Proc. 1st International Workshop on Agents and CyberSecurity - ACySE 14*, pp. 1–8, 2014.

[9] S. Garcia, M. Grill, J. Stiborek, and A. Zunino, "An empirical comparison of botnet detection methods," *Computers and Security*, vol. 45, pp. 100–123, September 2014.

[10] *Introduction to Cisco IOS NetFlow - A Technical Overview*. CISCO SYSTEMS, Inc. CISCO, 2012.

[11] *Lifelines*, Cam Davidson-Pilon, Copyright 2014.

[12] *GDP - NetFlow Collector*. Network Security Research, ©2016.

[13] *Fabric: Pythonic remote execution*, ©2016.

[14] Norman, Geoffrey R. and David L. Streiner. *Biostatistics: the bare essentials*. 3rd ed. Shelton, Conn.: People's Medical Pub. House, 2008. ISBN 9781550093476

[15] *GitHub, Fabric: Simple, Pythonic remote execution and deployment*, GitHub, 2016.

[16] C.D. Cam, *Lifelines*, 2014.

[17] *Stratosphere IPS*, Dataset, ©2015.

Vaclav Oujezsky (MSc) was born in Brno, Czech Republic. Post graduate student at Brno University of Technology, Department of Telecommunications, Senior Network Engineer at T-Mobile CZ, and currently at IBM CZ. Working actively on projects of security and transport networks at laboratory SIX. His research interests include implementation of evolutionary algorithm, Cisco, Python, VHDL, and converged networks. His topic of dissertation thesis is Converged Networks and Traffic Tomography by Using Evolutionary Algorithms.

Tomas Horvath (MSc) was born in Havirov, Czech Republic. He received his MSc. degrees in Telecommunications from the Brno University of Technology, Brno, in 2013. His research interests include passive optical networks (xPON) and optoelectronics. Currently, he is post graduate student at Brno University of Technology, Department of Telecommunications. His topic of dissertation thesis is Optimization Services in FTTx Optical Access Networks.

Vladislav Skorpil Vladislav Skorpil was born in Brno in 1955. He received the MSc. and CSc. degrees in Brno University of Technology (BUT). From 1980 to 1982 he worked as a designer for the telecommunication design office. He again entered the Department of Telecommunications of BUT in 1982 as a university teacher and he has been working in this department since that time. Now he is an associate professor and a vice-head of this department. He takes a keen interest in modern telecommunication systems. He is the author of about 153 international scientific papers and some manuals. He has cooperated on telecommunication projects such as digital transmission and switching systems, telecommunication broadband networks, data networks LAN and MAN, neural networks, grammatical algorithms, Quality of Service, data bit rate compression, etc. He is a member of international organisations IEEE and WSEAS.

ISSN 1805-5443