IEEE 2012 GLOBECOM
GLOBAL COMMUNICATIONS CONFERENCE, EXHIBITION & INDUSTRY FORUM

Issue 3
Wednesday, 5 December 2012

Dr. Henry Samueli of Broadcom Delivered Opening Keynote Address at IEEE GLOBECOM 2012

Immediately following the Tuesday morning's opening ceremonies, Dr. Henry Samueli, Co-founder, Chairman and CTO of Broadcom Corporation offered the conference's first keynote with his presentation titled "Connecting Everything: Dream Becomes Reality." Introduced by IEEE GLOBECOM 2012 Keynote Chair Mahmoud Daneshmand, Dr. Samueli spoke at length about Broadcom's beginnings dating back to two decades ago, the ensuring paradigm shifts that have produced "more connected devices then people on the planet" and the underlying theme that chip development is the "key innovation driving the connected world."

After reflecting on Moore's Law, he then reflected on the semiconductor industry's growth, which grew by a factor of one million over the past 40 years and was kicked off when IBM legitimized the personal computer, transforming the consumer electronics market in 1983. Other significant milestones that coincided with Broadcom's launch and continued growth since 1991, according to Dr. Samueli, were key technology breakthroughs encompassing digital receiver technology, high-speed digital processing and the introduction of the first cable-tv receivers in 1996.

"Now," said Dr. Samueli, "We are in the midst of a video and multimedia evolution that will literally digitize the entire signal." For instance, digital tv will grow by a factor of four as 2160p (4K x 4K) displays replace today's 1080p standard. Another will be the advance of broadband distributed throughout the home and the merger of consumer electronics with computer technologies to create whole-home networking backed by client-server type technologies available throughout the house.

Over the next 15 years, Dr. Samueli also elaborated on the rise of 100 Gbps broadband access speeds and home network rates that will combine with seamless user interfaces operated through voice and gesture inputs. Holographic projections will also become the norm in 2027, enabling users to manipulate objects in 3D space, while smartphones will evolve to desktop computer performance levels within only the next few years. By 2015, mobile Internet usage will overtake desktops with smartphones use growing four times faster than overall phone growth. This includes predictions based on present patterns that have shown "the average American already checking his or her smartphone 40x a day."

As for the near future, Dr. Samueli spoke of additional innovations that will revolutionize healthcare delivery through the use of wireless applications providing 24/7 healthcare monitoring and a new fleet automobiles that will literally become "mobile living rooms," integrating GP3 and WiFI to not only advance the safety of moving vehicles, but incorporate autonomous driving technologies allowing cars to drive themselves. Furthermore, Dr. Samueli concluded by stating that "ultra-low-power sensors will be everywhere," universally connected and readily accessed through images, touch, audio and motion operating at mobile device speeds exceeding 1 Gbps. In addition, ubiquitous broadband connectivity will become commonplace with seamless access to the cloud available nearly everywhere in the world.

TABLE OF CONTENTS

PROGRAM SPOTLIGHT

Keynote Session
Wednesday, 5 December 2012 • 08:00 – 09:30
Center Ballroom/North Ballroom A/B

Vinton Cerf

Vice President & Chief Internet Evangelist
Google

Internet Challenges 2012-2020

Security, Scale, Internet(s) of Things, Privacy, Reliability, Frameworks for international business, law enforcement and provision of safety in online environments are some of the topics to be addressed during this keynote talk.

Krish Prabhu

President, AT&T Labs and Chief Technology Officer

Connected Life: the Future of Global Communications

Advances in mobile broadband, the cloud, smart devices, user interfaces, and insights are coming together to fundamentally change the nature of the way applications are developed and used. This talk presents a vision of a "Connected Life" and describes work that is underway in AT&T's Labs to realize this vision. To cope with massive growth in network data traffic, mobile broadband networks are evolving into heterogeneous networks that seamlessly knit together multiple network technologies. To enable an ideal customer experience from anywhere at any time, and to better adapt to demand, services will be dynamically offered from a ubiquitous cloud infrastructure. Finally, innovation in devices and user-interfaces will deliver powerful new personalized experiences, providing users more ease, flexibility, and enjoyment.

IF16: Executive Forum: Data Infrastructure and Services
Wednesday, 5 December 2012 • 10:00 – 12:00
South Ballroom A

Sponsored by Making Light Work Lighter **General Photonics**

With traffic continuing to grow due to mobile, video and cloud services, carriers face significant challenges on how to upgrade and re-architect their networks. In this panel, the executives will discuss network architecture approaches, transport systems and the component trends that will enable the industry to achieve cost-effective, high flexible and high bandwidth data infrastructure and services

Invited Guest Speakers:
Joe Berthold, Network Architecture, CIENA Corporation, USA
Content-Centric Network Architecture

Christoph Glingener, CTO, Adva, Germany
From Static to Software Defined Optical Networks

Wupen Yuen, SVP, Product & Technology Development, NeoPhotonics, USA
Software-Defined Optical Networks Enabled by Photonic Integrated Circuits

Hamid Ahmadi, VP & Head, Advanced System Engineering Lab, Samsung Information Technology America, USA (Keynote)
Networking Trends In Mobile Computing

Geoffrey Mattson, VP Architecture, Juniper Networks, USA
Mutli-domain SDN and Network Evolution


Joe Berthold


Christoph Glingener


Wupen Yuen


Hamid Ahmadi


Geoffrey Mattson

PROGRAM SPOTLIGHT

N2Women-WiCE Lunch and Panel Discussion

Wednesday, 5 December 2012 • 12:00 – 13:30
Redondo Room, Disney's Paradise Pier Hotel

Prof. Brandt-Pearce
University of Virginia

Prof. Raffaelli
University of Bologna

Prof. Sarah Kate Wilson
Santa Clara University

Topics
- Attracting women in computing and computer science
- The barriers facing women to enter in scientific career
- Women's situation in the area of research in ten years

- N2Women is an ACM SIGMOBILE program that is supported by IEEE Communications Society, Microsoft Research and HP Labs.
- WiCE is a committee of women in communications engineering in IEEE Communications Society.
- This meeting has been generously supported by IEEE GLOBECOM 2012.

Organizers:
Sanaz Barghi (University of California, Irvine)
Sahar Hoteit (University of Pierre and Marie Curie, France)

Banquet Keynote

Wednesday, 5 December 2012 • 19:00 – 23:00
Center Ballroom

Steven Rosenbaum

Producer

Steven Rosenbaum (born 1961) is an American television producer and Filmmaker best known as the creator of MTV News UNfiltered.

He is the author of Curation Nation curationnation.org published by McGrawHill Business on 11 March 2011. The book explores the emerging phenomenon of human organization and publishing of content. Reviewer Shel Holtz said: "This groundbreaking book levels the playing field, giving your business equal access to the content abundance presently driving consumer adoption of the Web."

He is the founder of Magnify.net, where people can integrate user-generated video, video that they produce, or video that they discover into a website with social networking features.

In 2011, Rosenbaum created The 9/11 Memorial: Past, Present, and Future **www.911MemorialApp.com** a hybrid book and multi-media offering for the Apple iPad. The so-called AppBook received both critical acclaim and criticism for not supporting android devices. Rosenbaum is New York City's first Entrepreneur at Large working with New York's startup community and NYCEDC.

Rosenbaum was named Purdue University Science Journalism Laureate in 2011. Rosenbaum won an Emmy Award for BROADCAST: New York and then created the series MTV News UNfiltered for MTV, an early example of viewer-generated content in broadcast. "News Unfiltered" encouraged people film their own stories.

Rosenbaum directed the documentary feature 7 Days In September, a look at 9/11 and the week after. Rosenbaum also created the CameraPlanet 9/11 Archive, an archive of footage from September 11 and its aftermath. Rosenbaum has received 2 Emmy Awards, 6 New York Festival's World Medals, 4 CINE Golden Eagles and 6 Telly Awards. CameraPlanet holds a large archive of videos from 9/11, mainly consisting of home videos taken by professionals and amateurs in September 2001.

Other producer credits include the Animal Planet series Dog Days and VH1's A Night With. CameraPlanet Chief Correspondent Peter Arnett reported from Afghanistan and Pre-War Iraq.

In 1998, Rosenbaum created and funded a video journalism program at Columbia University's Graduate School of Journalism and founded the BNN Scholarship for Columbia University journalism students. Rosenbaum also serves as a member of Board of Advisors for a nonprofit organization, **www.ClassWish.org**.

CAMBRIDGE

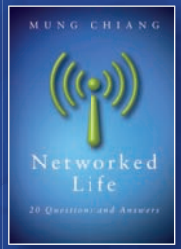
Presenting New and Featured Books in Communications Engineering!

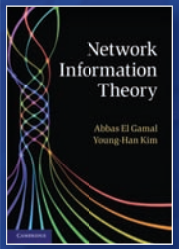
VISIT BOOTH #19 *and* SAVE 20%

Networked Life
20 Questions and Answers

Mung Chiang

September 2012
Hb: 978-1-107-02494-6: 488 pp: List Price: $45.00





Network Information Theory

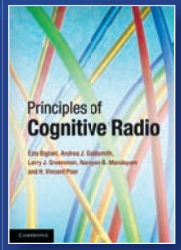
Abbas El Gamal *and* Young-Han Kim

January 2012
Hb: 978-1-107-00873-1: 714 pp: List Price: $85.00

Principles of Cognitive Radios

Ezio Biglieri, Andrea J. Goldsmith, Larry J. Greenstein, Narayan Mandayam, *and* H. Vincent Poor

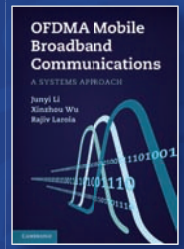
December 2012
Hb: 978-1-107-02875-3: 352 pp: List Price: $95.00



OFDMA Mobile Broadband Communications
A Systems Approach

Junyi Li, Xinzhou Wu, *and* Rajiv Laroia

January 2013
Hb: 978-1-107-00160-2: 528 pp: List Price: $85.00



Green Radio Communication Networks

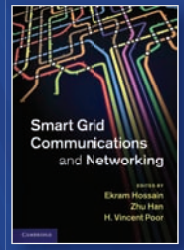
Edited by Ekram Hossain, Vijay K. Bhargava, *and* Gerhard P. Fettweis

August 2012
Hb: 978-1-107-01754-2: 440 pp: List Price: $125.00

Smart Grid Communications and Networking

Edited by Ekram Hossain, Zhu Han, *and* H. Vincent Poor

June 2012
Hb: 978-1-107-01413-8: 500 pp: List Price: $145.00



Prices subject to change.

View our entire catalog at **www.cambridge.org/engineering**

800.872.7423

@CambUP_engineer

CAMBRIDGE UNIVERSITY PRESS

EVENTS OF THE DAY

08:00 – 09:30
KEYNOTE SESSION
Vinton Cerf, Google
Krish Prabhu, AT&T
Center Ballroom/North Ballroom A/B

09:30 – 10:00
COFFEE BREAK / South Exhibit Hall
Prize Drawing (must be present to win)

10:00 – 12:00
INDUSTRY FORUMS
IF16: Executive Forum: Data Infrastructure & Service / South Ballroom A
IF17: Next Generation Cellular & Satellite Communication I / North Ballroom A

TECHNICAL SESSIONS
AHSN04: Wireless Sensor Network Routing II / North Exhibit Hall A
AHSN13: DTN & Opportunistic Networking / North Exhibit Hall B
CISS04: Internet Security I / North Exhibit Hall C
CISS10: Information Security and Cryptography / North Exhibit Hall D
CogRN04: MIMO & Cooperative Relaying Cognitive Radio Networks / Magic Kingdom Ballroom 4
CQ04: Service & Application on Communication Networks / North Exhibit Hall F
CSSM04: Mobile Service and Service Platform / North Exhibit Hall G
CT03: Network Coding / North Exhibit Hall H
NGNI04: Network Virtualization / North Exhibit Hall I
ONS02: Wireless Optical Communications and Networks / North Exhibit Hall J
SAC-GNCS4: Analysis for Green Wireless Communications / Castle A
SPC05: Coding and Decoding / Castle B
SPC06: COMP / Magic Kingdom Ballroom 3
WC10: Relay Technologies: Performance Analysis & Relay Selection / Castle C
WC11: Network Coding I / Monorail A
WC12: MIMO Systems: Transmission & Detection / Monorail B
WC13: Cellular Networks / Monorail C
WN07: 802.16 & LTE Networks / Magic Kingdom Ballroom 1
WN08: Wireless Sensor Network Design / Magic Kingdom Ballroom 2

POSTER SESSIONS / South Exhibit Hall
SPC01P: Signal Processing for Communications II
WC01P: Wireless Communications I
WC02P: Wireless Communications II
WC03P: Wireless Communications III

12:00 – 13:30
LUNCH / On Your Own

13:30 – 15:30
INDUSTRY FORUMS
IF18: Next Generation Cellular & Satellite Communication II / North Ballroom A
IF20: Funding Innovation & Technology Incubator Process in Telecom Italia & European Commission / South Ballroom A
IF21: Communication Investment in a Global Economy / North Exhibit Hall E

TECHNICAL SESSIONS
AHSN05: Localization & Tracking / North Exhibit Hall A
AHSN14: Security Issues / North Exhibit Hall B
CISS05: Internet Security II / North Exhibit Hall C
CogRN05: Spectrum Sensing I / North Exhibit Hall D
CQ05: Traffic Modeling & Performance Evaluation / Castle A
CSSM05: Cloud & Social Networking / North Exhibit Hall F
CT04: Interference Management / North Exhibit Hall G
NGNI05: Resource Allocation & Routing in Next Generation Networks / North Exhibit Hall I
SAC-DS01: Coding and Signal Processing for Data Storage / North Exhibit Hall H
SAC-GNCS5: Green Data Centers & Cloud Computing / North Exhibit Hall J
SPC07: Signal Processing for Communications I / Castle B
WC14: Relay Technologies: Decode-and-Forward / Castle C
WC15: OFDMA / Monorail A
WC16: MIMO Systems: Performance Analysis / Monorail B
WC17: Routing & Scheduling / Monorail C
WN09: Cellular Networks II / Magic Kingdom Ballroom 1
WN10: Medium Access Control / Magic Kingdom Ballroom 2

POSTER SESSIONS / South Exhibit Hall
AHSNP: I
CQ10P: Topics in QoS, Reliability & Modeling
CSSMP: Communications & Multimedia Service
ONS05P: Miscellaneous Topics in Optical Networks & Systems
WN18P: Topics in Wireless Networking

15:30 – 16:00
COFFEE BREAK / South Exhibit Hall
Prize Drawing (must be present to win)

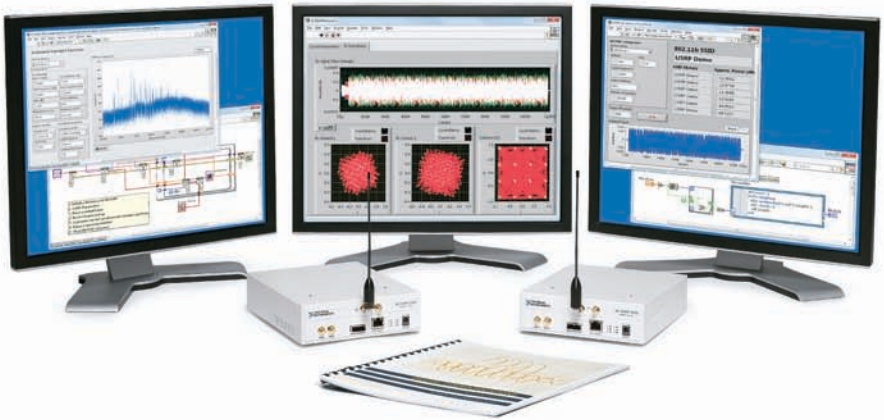
16:00 – 18:00
INDUSTRY FORUMS
IF19: Smart Data Pricing / South Ballroom A
IF22: Education Forum / North Ballroom A
IF30: IP Based Business Models & Tech Trends in Entrepreneurs / North Exhibit Hall E

TECHNICAL SESSIONS
AHSN06: Cognitive Networking / North Exhibit Hall A
AHSN15: MAC / North Exhibit Hall B
CISS06: Security in Cyber-Physical Systems / North Exhibit Hall C
CogRN06: Modeling & Analysis of Cognitive Radio Networks / North Exhibit Hall D
CQ06: Traffic Control / Magic Kingdom Ballroom 4
CSSM06: Security & Multimedia Streaming / North Exhibit Hall F
CT05: Coding Techniques / North Exhibit Hall G
NGNI06: P2P & Content Centric Networks / North Exhibit Hall H
SAC-ASN2: System, Architectures & Algorithms / North Exhibit Hall I
SAC-GNCS6: Physical Layer Designs for Green Communications / North Exhibit Hall J
SAC-SSC01: Satellite & Space Networking / Castle A
SPC08: MIMO II / Castle B
WC18: Relay Technologies: Amplify-and-Forward / Castle C
WC19: Network Coding II / Monorail A
WC20: OFDM I / Monorail B
WC21: Beamforming / Monorail C
WN11: Power Control & Resource Management / Magic Ballroom Kingdom 1
WN12: Vehicular Networks / Magic Ballroom Kingdom 2

POSTER SESSIONS / South Exhibit Hall
AHSNP: II
CogRN12P
CT10P

19:00 – 23:00
BANQUET / Center Ballroom

Flexible, Affordable Software Defined Radio



Rapidly prototype powerful wireless communications systems for research and education combining an affordable software defined radio platform with NI LabVIEW system design software.

Learn more about National Instruments SDR solutions at Booth 9.

>> Join *Digital Communications Lab Manual* author Dr. Robert Heath, and other distinguished speakers at the Wednesday Education Forum (IF22) panel discussion.

NATIONAL INSTRUMENTS™

PROGRAM UPDATES

The following are updates to the program guide found in your badge holder. These updates appear in the online final program.

Wednesday, 5 December 2012
IF17: Next Generation Cellular & Satellite Communication I
from 10:00 – 12:00 will now be held in North Ballroom A.
IF18: Next Generation Cellular & Satellite Communication II
from 13:30 – 15:30 will now be held in North Ballroom A.
IF22: Education Forum
from 16:00 – 18:00 will now be held in North Ballroom A.

Thursday, 6 December 2012
IF25: Cable Industry Access Technology
from 16:00 – 18:00 will now be held in North Ballroom A.
IF28: Optical Wireless Access
from 13:30 – 15:30 will now be held in North Ballroom A.
IF23: Lightning Talks
from 16:00 – 18:00 will now be held in North Ballroom A.

Friday, 7 December 2012
T9: Opportunistic Communication
from 09:00 – 12:00 will now be held in Magic Kingdom Ballroom 1/4.
T12: Cooperative Spectrum Sensing
from 14:00 – 17:00 will now be held in Magic Kingdom Ballroom 1/4.

FEATURED ARTICLE

Cellular Bonding for HD Quality Live Video Transmission

By **Rony Ohayon**, CTO, LiveU

There comes a time in every innovative technology sector when the question changes from whether to use the technology to how to deploy it? From a cellular bonding perspective the London 2012 Olympics and US Presidential Election marked this point with hundreds of units used by the world's media for live video coverage.

Over the last five years, cellular/IP bonding has changed the transmission space significantly. New patented algorithms, advanced video encoders, 3G deployment and emerging 4G/LTE networks have provided a resilient, cost-effective alternative to streaming SD and HD video via traditional satellite links. Today, more and more broadcasters and online media use cellular-bonded technology for cost-effective live video transmission from any location, combining any combination of cellular technologies and networks, including 2.5G, 3G, 4G LTE, Wi-Fi and WiMAX, for reliable, HD (even up to 3D) video uplinks.

The Bonding Challenge
In order to provide high quality live video uplink transmission, cellular-based technology has succeeded in overcoming the Quality of Experience (QoE) challenge. While high-quality video experience relies on smooth and uninterrupted video delivery, cellular links are inherently unstable and fluctuate continuously. Transmitting video over any such single link may result in black screens, video breaks, pixelization, jitters, audio problems, lost lip-sync etc., even over 4G networks and from stationary locations. Parameters that impact the experience and can change in a millisecond include: uplink bandwidth, uplink latency, loss rate or sharp BW change, out of order packets, or all of them together.

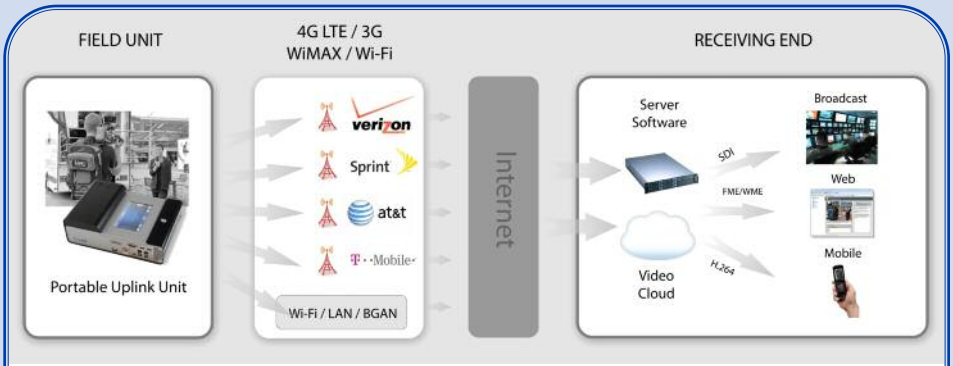
Cellular bonding technology bridges the gap between the desired video experience and inherent cellular behavior.

Bonding Architecture
Optimum bonding solutions maximize the Quality of Experience (QoE) by leveraging available network resources. The uplink backpack or handheld device continuously, and in real time, monitors all available links and adaptively controls the content generation, protection, and multi-link scheduling functions. Instead of relying on a single unreliable link with a single point of failure, multi-link bonding technology improves the reliability, data throughput, and service coverage, minimizing the inherent risks of losing connectivity. The device controls the available links and determines how best it can utilize each of them.

On the transmission side, the device modifies the H.264 video encoder parameters in real time, such as the frame rate, quality, and resolution, optimizing transmission to the momentarily available bandwidth of all the links. To compensate for, and recover from, variable rate packet loss over the cellular network, the content is adaptively protected using a smart multi-link Forward Error Correction (FEC) algorithm that takes into consideration the statistical behavior of the links. The algorithms then transmit some of the H.264 packets over each of the multiple cellular modems according to their monitored momentary performance, predicted behavior, type of packets, etc.

On the receiving side, the video server combines the multiple video streams and delivers the reconstructed video stream to the TV studio or online distribution platform. Bonding several cellular links together minimizes the inherent risks while achieving the desired or greater performance.

continued next page >>



LiveU's Cellular Bonding Workflow

Impact of 4G LTE Networks
Although 4G LTE brings the promise of higher peak bandwidth and shorter delays to bonded cellular video transmission, single-modem video delivery devices are still inherently unstable and may well experience performance fluctuations, loss of transmission and the inability to go live. This is usually due to network overload, as operators start to promote networks more intensely, advertised vs. actual performance and slower 4G roll-out outside city centers.

LiveU multi-link solutions, which use 4G LTE along with other available networks, allow broadcasters, online video professionals and other sectors to enjoy the benefits of both the 4G and 3G worlds. While harnessing the extra bandwidth and shorter delay provided by the LTE network, bonded solutions overcome LTE difficulties with 4G/3G technology switching. A properly-designed LTE-bonding system automatically switches a greater percentage of the transmitted video bandwidth over to the 3G networks in relevant areas without, for example, succumbing to broadcast breakdowns because of relying too much on any single LTE link.

Indeed for many years to come, multi-link backpacks and handheld uplink devices that simultaneously bond 3G and 4G technology will see the best results.

Where do we go from here?
While continuing to improve the algorithms, we're also looking into other markets and their special requirements. For example, when transmitting live from Afghanistan or Haiti, some customers have bonded two BGAN satellite links to achieve the required bandwidth.

LiveU has recently launched an iPhone/iPad application that bonds its Wi-Fi and 3G/4G modem to generate the extra bandwidth while also providing the added value coming from this QoE-guided traffic offloading. Getting ready for higher quality video, such as 4K video, or multi-HD channels transmitted over the same bonding channel, are some other examples for the future.

Summary
Cellular-bonded technology has entered the mainstream, used for almost every major event around the world. It's even proven itself as the most effective transmission technology in the most extreme weather conditions, such as recent Hurricane Sandy coverage. To a great extent, LiveU has led this space, moving from a product-based approach to one that concentrates on solutions, offering broadcasters, online media professionals, government, law enforcement and enterprise organizations an even greater number of devices for transmitting live video coverage, including mobile app and laptop solutions.

With the increased deployment of 4G LTE and continued technological advancements, cellular uplink technology will have an even greater role going forward in international news and event coverage.

ciena : the network specialist

behind every smart network… is a ciena solution.

The intelligent choice.

Ciena's OPn network architecture helps you economically scale your network over wide areas—with industry-leading optical and lean packet capabilities, software automation, intelligent control planes, performance-on-demand cloud networking, and unified network management.

Visit booth #10 or Ciena.com to learn more

EXHIBIT HALL

Don't miss the Poster Sessions
held only today in the Exhibit Hall.

Book publishers are offering a special 20%
conference discount on all books on display.
Visit Cambridge University Press (Booth #18), Springer (Booth #19) and Wiley-Blackwell (Booth #7) for more information.

Stop by IEEE GLOBECOM 2013 (Booth 21), IEEE GLOBECOM 2014 (Booth #1), IEEE ICC 2013 (Booth #15), IEEE ICC 2014 (Booth #2) and IEEE ICC 2015 (Booth #3) to learn more upcoming 2013, 2014 and 2015 IEEE GLOBECOM and ICC conferences

Check out the monitor in the Exhibit Hall
showcasing the #GLOBECOM Twitter Wall, Yammer comments and ComSoc Presidents' Recollections Video, which can also be found at http://www.ieee-globecom.org/presidents/.

Prize drawings will be held during the morning and afternoon coffee breaks in the Exhibit Hall. Drop your ticket (included in your registration packet) or business card in the ticket tumbler on the stage in the Exhibit Hall. One prize per attendee. Must be present to win.

TUESDAY'S PRIZE DRAWING WINNERS

IEEE GLOBECOM 2012 Officially Opened on Tuesday Morning with the Remarks of IEEE GLOBECOM 2012 Executive Chair Pierre Perra & Conference Committee Members & Organizers

IEEE GLOBECOM 2012 officially commenced Tuesday morning with the welcoming and introductory remarks of IEEE GLOBECOM 2012 Executive Chair Pierre Perra. During his comments, Executive Chair Perra thanked the patronage of many of the conference's sponsors including Ciena, the platinum patron as well as silver and bronze patrons like Samsung, AT&T, Google, Broadcom, Huawei, Ericsson, Cisco, EMC2 and Qualcomm. Also thanked were the entire IEEE GLOBECOM 2012 organizing committee and exhibitors like Ranplan Wireless Net Design, Cambridge University Press and Springer.

Following these comments, IEEE ComSoc President Vijay Bhargava spoke about the society's 60th anniversary and urged everyone in attendance to view the commemorative video assembled by Steve Weinstein, Chair of ComSoc's Communications History Committee, currently available on display in the conference exhibition hall. The IEEE GLOBECOM Technical Program Chair Zhensheng Zhang then offered a brief overview of this year's technical program composed of 12 symposia, 21 workshops and 11 tutorials. This included thanking the conference's 46 symposium chairs for their stellar efforts as well as citing the receipt of 2,560 paper submissions as representation of the overall regard held by researchers and scientists worldwide for this premier event.

IEEE GLOECOM 2012 Industry Forum & Exhibition Chair Narisa Chu then also then thanked all her colleagues for their hard work in making this year's comprehensive forum agenda an esteemed success. This includes the presentation of 32 sessions specifically devoted to industry and five keynotes dedicated to the main themes of cloud computing, next generation wireless, VINTage Internet and technology financing. She also cited numerous firsts for this annual event, which included the give-away of games and books at the "Digital Games" Industry Tutorial and the JPL tour highlighting the disruption tolerant networks used in the Mars Rover.

After the keynote of Henry Samueli of Broadcom, the ceremonies then proceeded with the "Best Paper Awards, which were announced by IEEE GLOBECOM 2012 Chair Perra and presented by IEEE ComSoc Vice President of Conferences Abbas Jamalipour. Among those honored were:

Igor Bisio Stefano Delucchi, **Fabio Lavagetto** and **Mario Marchese** for their paper titled "Capacity Bound of MOP-based Allocation with Packet Loss and Power Metrics in Satellite Communications Systems"

Liangbin Li, **Hamid Jafarkhani**, **Syed Ali Jafar** for their entry on "Towards the Feasibility Conditions for Linear Interference Alignment with Symbol Extensions: A Diversity Constraint"

Lin Zhang, **Guodong Zhao**, **Gang Wu**, **Zhi Chen** for 'Proactive Channel Gain Estimation for Coexistence between Cognitive and Primary Users"

Mariana Dias; **Nelson L. S. da Fonseca** for their paper on "A Robust WiMAX Scheduler for EPON-WiMAX Networks"

Marco Levorato, **Sunil Narang**, **Urbashi Mitra** and **Antonio Ortega** for their submission on "Reduced Dimension Policy Iteration for Wireless Network Control via Multiscale Analysis"

A. M. Rashwan, **A-E M. Taha** and **H.S. Hassanein** for "Benchmarking Message Authentication Code Functions for Mobile Computing"

Marcin Niemiec and **Andrzej R. Pach** for their paper titled "The measure of security in quantum cryptography"

Mohammad Noshad and **Maite Brandt-Pearce** for their submission on "Multilevel Pulse-Position Modulation Based on Balanced Incomplete Block Designs"

Jin Zhang, **Hao Tang**, **Dawei Chen**, **Qian Zhang** for deStress: Mobile and Remote Stress Monitoring, Alleviation, and Management Platform

Qian (Clara) Li, **Rose Qingyang Hu**, **Yi Qian** & **Geng Wu** for their entry titled "A Proportional Fair Radio Resource Allocation for Heterogeneous Cellular Networks with Relays

Sailesh Bharati & **Weihua Zhuang** for the paper on "Performance Analysis of Cooperative ADHOC MAC for Vehicular Networks"

Huseyin Haci, **Huiling Zhu** & **Jiangzhou Wang** for the submission named "Novel Scheduling for a Mixture of Real-time and Non-real-time Traffic"

Camillo Gentile, **Fabien Valoit** & **Nader Moayeri** for their paper on "A Raytracing Model for Wireless Propagation in Tunnels with Varying Cross Section"

Lu Wang, **Kaishun Wu**, **Jiang Xiao** and **Mounir Hamdi** for their entry about "FCM: Frequency Domain Cooperative Sensing and Multi-channel Contention for CRAHNs"

Maram Bani Younes, **Graciela Roman Alonso** & **Azzedine Boukerche** for the paper on "A Distributed Infrastructure-Based Congestion Avoidance Protocol for VANETs"

Annual Awards Luncheon Held at IEEE GLOBECOM 2012 on Tuesday Afternoon

An annual tradition involving hundreds of attendees, the Awards Luncheon at IEEE GLOBECOM 2012 began on Tuesday afternoon with Awards Chair Andreas Molisch welcoming all the participants to this year's conference andpaying homage to the tremendous efforts of today's distinguished honorees. During these remarks, he also cited the exhaustive selection process of the awards committee, which includes the reading of 30 – 40 papers by each member.

Throughout the proceedings, Awards Chair Molisch then announced each recipient name as IEEE ComSoc President Vijay Bhargava congratulated the individuals on stage in front of a full room of colleagues in the Grand Ballroom of the Fantasy Tower in the Disneyland Hotel. Among the Career and Service Award winners at IEEE GLOBECOM 2012 were:

Sergio Benedetto, who received the IEEE Communications Society Donald W. McLellan Meritorious Service Award "For outstanding and sustained contributions to the Communications Society's technical activities, publications enhancement and global member relations"

Niklas Zennstroem and **Janus Friis**, who were awarded the IEEE Communications Society Distinguished Industry Leader Award "For the distinguished leadership provided in co-founding, promoting, and leading Skype, a revolutionary business and technology, to a prominent position in the global market for low cost, peer-to-peer, Internet Protocol communications"

Hikmet Sari, who was selected for the IEEE Communications Society Harold Sobol Award for Exemplary Service to Meetings & Conferences "For 10 years of outstanding contribution to the organization and technical management of IEEE Communications Society's flagship conferences"

Nelson Fonseca, who was given the IEEE Communications Society Joseph LoCicero Award for Exemplary Service to Publications "For outstanding service to IEEE Communications Society publications as Editor-in-Chief of IEEE Communications Surveys and Tutorials, Editor-in-Chief of the IEEE Communications Society Electronic Newsletter and Editor of Global Communications Newsletter"

Donald Cox, who was honored with the IEEE Communications Society Edwin Howard Armstrong Achievement Award "For contributions, as a researcher, manager, and teacher, to the field of radio communications, in particular, cellular systems, communications satellites, and universal portable wireless services"

Veena Rawat, who was given the IEEE Communications Society Award for Public Service in the Field of Telecommunications "For outstanding public service through negotiating at international level access to radio frequency spectrum essential for wireless communication services and promoting a generation of youth, in particular women to study science and engineering"

Stephen Alexander, who was provided the IEEE Communications Society Industrial Innovation Award "For innovative industry contributions to optical communications technologies, systems and architectures"

Jin Li, who was provided 2012 IEEE Fellow honors "For contributions to multimedia delivery, compression and storage for real-time communication"

In addition to the aforementioned honorees, also cited by the IEEE Communications Society were this year's Prize Paper Awards Recipients, which included:

Alexander Afanasyev, **Neil Tilley**, **Peter Reiher** & **Leonard Kleinrock**, who given The 2012 IEEE Communications Society Best Tutorial Paper Award for their paper titled "Host-to-Host Congestion Control for TCP," IEEE Communications Surveys & Tutorials, Vol.12, No.3, Third Quarter 2010, pp. 304-342

Eric Torkildson, **Upamanyu Madho** & **Mark Rodwell**, who were awarded The 2012 IEEE Marconi Prize Paper Award in Wireless Communications for their submission on "Indoor Millimeter Wave MIMO: Feasibility and Performance," IEEE Transactions on Wireless Communications, Vol.10, No.12, December 2011, pp. 4150-4160

Andrea Conti, **Wesley M. Gifford**, **Moe Z. Win** & **Marco Chiani**, who received The 2012 Stephen O. Rice Prize in the Field of Communications Theory for their paper on "Optimized Simple Bounds for Diversity Systems," IEEE Transactions on Communications, Vol. 57, No. 9, September 2009, pp. 2674-2685

Moe Z. Win, **Andrea Conti**, **Santiago Mazuelas**, **Yuan Shen**, **Wesley M. Gifford**, **Davide Dardari** & **Marco Chiani**, who were given The 2012 IEEE Communications Society Fred W. Ellersick Prize for their work on "Network Localization and Navigation Via cooperation," IEEE Communications Magazine, Vol. 49, No.5, May 2011, pp. 56-62

Shafayat Abrar & **Asoke K. Nandi**, who were given The 2012 IEEE Communications Society Heinrich Hertz Award for Best Communications Letter for their work on "Adaptive Minimum Entropy Equalization Algorithm," IEEE Communications Letters, Vol. 14, No.10, October 2010, pp. 966-968

Pulkit Grover, **Kristen Woyach** & **Anant Sahai**, who received The 2012 IEEE Communications Society Leonard G. Abraham Prize Paper Award in the Field of Communications Systems for their submission titled "Towards a Communication-Theoretic Understanding of System-Level Power Consumption," IEEE Journal on Selected Areas in Communications, Vol. 29, No. 8, September 2011, pp.1744-1755

Alberto Rabbachin, Tony Q.S. Quek, Hyundong Shin & Moe Z. Win, who were provided The 2012 IEEE Communications Society William R. Bennett Prize in the Field of Communications Networking for their entry on "Cognitive Network Interference," IEEE Journal on Selected Areas in Communications, Vol. 29, No. 2, February 2011, pp. 480-493

Siavash M. Alamouti, who was honored with The 2012 IEEE Communications Society Award for Advances in Communication Outstanding Paper on New Communications Topics for his entry titled "A Simple Transmit Diversity Technique for Wireless Communications," IEEE Journal on Selected Areas in Communications, Vol. 16, No. 8, October 1998, pp. 1451-1458.

YESTERDAY'S NEWS

IEEE GLOBECOM 2012 Executive Forums Commenced on Tuesday Morning with "New Technologies to Watch" Session

The IEEE GLOBECOM 2012 technical and business information program began on Tuesday morning with the first of three full days of industry forums, technical presentations, keynotes and panels dedicated to the latest advances in the entire range of communications. Highlighting this agenda was the Executive Forum titled "New Technologies to Watch" held on Tuesday morning and featuring the new dynamic capabilities and applications currently under development by the industry's leading corporations and research institutions.

Among the session's expert presenters was Dr. Chen Chang, CEO of BeeCube Inc., who started his presentation titled "So Many Users, So Many Opportunities, So Little Spectrum, So Little Time" by asking "What is driving the invention of these new technologies?" Without hesitation, he cited the convergence of the wireless mobile world with E-commerce that has currently produced more than one billion global smartphone users as well as $1 billion in sales on Black Friday within the United States and $4 billion in China on November 11, 2011.

Following these comments, Dr. Chang then spoke about the challenges of turning the network offering the latest communications, computing and storage capabilities into user-friendly computers with ready access to information any time or day. According to him, the real culprit is not only the lack of spectrum space, but also the basic inability to even decide how to use the spectrum more effectively. This includes providing bandwidth at a lower cost and creating an "all digital world" emphasizing the introduction of flexible, programmable platforms that emerge from the lab to the field in record times with features and gimmicks that consumers want.

Afterwards, Patrick Diamond, founder of Patrick Diamond Consulting, discussed "Techniques for Precise Time Transfers Over Optical Networks." In his talk, Diamond talked about the "real down-home engineering" and global importance involved in providing industries such as banking, transportation and communications with wireless access to precise synchronized time via optical paths. As an example, he noted that 90 percent of all equities trades are authenticated by time/day stamps measured in microseconds and total more than 22 billion messages in the U.S. alone. Without this capability in October 2012, the New York Stock Exchange was forced to cease operations due to the affects of Hurricane Sandy in New York and New Jersey and the damage inflicted on the area's GPS antennas.

As a way to overcome the spoofing of GPS devices, which are "totally incapable of knowing they're being jammed," Diamond reviewed the benefits of the IEEE 1588-2008 Precision Time Protocol and its proven capabilities for preventing jamming and spoofing in precise time and frequency transfers. This includes transporting a time stamp to reference sources in a packet, extracting the stamp from networks and delivering a precise copy to end users utilizing LTE networks.

Other presentations offered throughout forum were the discussions provided by Y.K. park of OE solutions, who spoke of "Intelligent Optical Transceivers for Efficient Telecom Network Operations" and Dean Sirovica of Huawei Technologies, who highlighted the process of innovation and his company's current R&D efforts.

IEEE GLOBECOM 2012 BEST PAPERS

On the following pages, the 3 of 15 best papers featured are from Symposia on Communications and Information System Security, Optical Networks and Systems and Communication Software, Services and Multimedia Applications.

Multilevel Pulse-Position Modulation Based on Balanced Incomplete Block Designs

Mohammad Noshad and Maïté Brandt-Pearce
Charles L. Brown Department of Electrical and Computer Engineering
University of Virginia
Charlottesville, VA 22904
Email: mn2ne@virginia.edu, mb-p@virginia.edu

***Abstract*—In this paper, two new modulation schemes using multilevel pulse-position modulation (PPM) for application in unipolar optical wireless systems are presented. Balanced incomplete block designs (BIBD) are used for constructing the symbol alphabets. Each symbol is obtained by combining multiple codewords of a BIBD code. In one scheme the symbols have equal energies, and therefore, no threshold is needed to make a decision on the received signal. The other modulation has better performance yet higher complexity. Since cyclic BIBDs are used for constructing the symbols, the transmitters and receivers have simple structures, and can be implemented using shift registers. These schemes can achieve high spectral-efficiencies, and are therefore suitable for systems with bandlimited sources or highly dispersive channels, where intersymbol interference (ISI) has a significant impact on the performance. We also show that using the same receiver structure, the constellation size can be increased by including the complements of the codewords. The performance of the proposed schemes are compared to other modulation schemes for both LED-based non-dispersive and dispersive free-space optical (FSO) systems.**

***Index Terms*—Multilevel modulation, pulse position modulation (PPM), balanced incomplete block design (BIBD), free space optical (FSO) systems, spectral-efficiency**

I. Introduction

Free space optical (FSO) communications has recently attracted significant interest because of its huge unlicensed bandwidth and potential in providing high data-rates [1], [2]. Emerging applications, such as indoor visible light optical communications and non-line-of-sight (NLOS) ultraviolet (UV) communications [3], have made FSO communications more important than ever. Pulse position modulation (PPM) is considered the primary M-ary transmission technique for FSO links, since it can be implemented incoherently and does not need a threshold to make decisions at the receiver side, which is important in fading channels. Because of the low spectral-efficiency of PPM, dispersive channels cause interference between the time-slots. Therefore, low spectral-efficiency is the main limiting factor for PPM, which makes it vulnerable to intersymbol interference (ISI), and prevents it from being used in dispersive channels, such as in the applications mentioned above. Multipulse PPM (MPPM) has been proposed [4] to improve the spectral-efficiency of PPM by increasing the constellation size. In this paper, we propose two new multilevel pulse-position based modulation schemes to achieve higher spectral-efficiencies while simultaneously enforcing large minimum pairwise Hamming distances between symbols.

Various multilevel modulation schemes using a combination of PPM and pulse-amplitude modulation (PAM) have been proposed in the literature in order to improve the spectral-efficiency of pulse-position based modulations [5], [6], [7]. In these works, all combinations of PPM and PAM are considered as symbols, and therefore, the minimum distance between symbols is small. Moreover, the symbols in these schemes contain different energies, and hence the receiver requires a threshold value to make a decision, which is a disadvantage in fast-fading channels.

In [8], we propose a novel unipolar modulation scheme, called expurgated PPM (EPPM), as an alternative technique to PPM to improve the performance of peak-power limited M-ary communication systems. Balanced incomplete block designs (BIBD) are used as modulated symbols in order to increase the Hamming distance between symbols. Because of the cyclic structure of the BIBD codes, the transmitter and receiver have low complexity and can be implemented using shift registers. It is also shown that for the same receiver structure, by including the complements of the codewords a higher constellation size can be achieved.

In our proposed modulation schemes, the multilevel symbols are obtained as linear combinations of BIBD codewords, and therefore, all symbols have fixed weight. These techniques can be considered as multilevel forms of EPPM, and thus, we call them multilevel EPPM (MEPPM). We propose two constructions of MEPPM: one with a simpler decoder and no need for a threshold, and the other with better performance in exchange for a somewhat more complex detector. We also show that by including the complements of the BIBD codewords the constellation size can be increased significantly, without any change in the receiver structure. The proposed technique can achieve 75% higher spectral-efficiency compared to MPPM at a BER of 10^{-5}.

The rest of the paper is organized as follows. Section II describes the principles of the MEPPM schemes and the transmitter and receiver structures. The analytical symbol error probability of MEPPM is approximated in Section III using the union bound, and the spectral-efficiency is calculated for each scheme. Numerical results are presented in Section IV, and the spectral-efficiencies of our proposed multilevel schemes are compared with other modulations. Finally, conclusions are

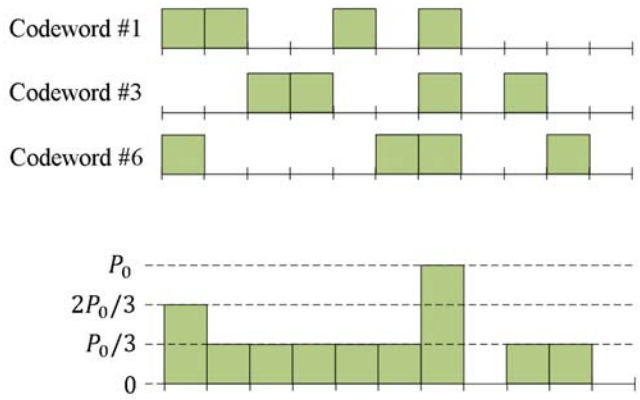


Fig. 1. A 4-level EPPM symbol constructed using codewords 1, 3 and 6 of a $(11, 4, 1)$-BIBD.

provided in Section V.

II. Principles of Multilevel EPPM

This section explains the principles of the multilevel EPPM (MEPPM) and its transmitter/receiver structures. In these schemes, similar to PPM, the symbol period is divided into Q equal time-slots. A unipolar L-level encoding is applied on the amplitude of the optical power in each time-slot. Hence, symbol k is denoted by $S_k = (s_{k1}, s_{k2}, \ldots, s_{kQ})$, where $0 \leq s_{ki} \leq L-1$.

We use the codewords of a BIBD code to construct the symbols of MEPPM. A BIBD code is composed of Q codewords, $\{C_1, C_2, \ldots, C_Q\}$, and each codeword has a length of Q, i.e., $C_j = (c_{j1}, c_{j2}, \ldots, c_{jQ})$ [9], $c_{ji} \in \{0, 1\}$, such that

$$\sum_{i=1}^{Q} c_{ji}c_{ki} = \begin{cases} K & ; j = k, \\ \lambda & ; j \neq k \end{cases}, \tag{1}$$

where K is the weight and λ is the cross-correlation of that code. We denote a BIBD code by $(Q,\ K,\ \lambda)$, and the following relation holds for its parameters [9]:

$$\lambda(Q-1) = K(K-1). \tag{2}$$

For our MEPPM, each symbol is obtained as the sum of N BIBD codewords from the same code, resulting in new length-Q codewords. We focus on cyclic BIBDs, for which the codewords are cyclic shifts of each other. To build symbol k, N codewords are chosen, denoted as C_{k_n}, $n = 1, 2, \ldots, N$, $k_n \in \{1, 2, \ldots, Q\}$, resulting in $S_k = (s_{k1}, s_{k2}, \ldots, s_{kQ})$, where s_{ki} can be obtained as

$$s_{ki} = \sum_{n=1}^{N} c_{k_n i}. \tag{3}$$

According to this definition, the symbols of a MEPPM constellation have equal weight, where the weight of each symbol is NK. Fig. 1 shows the generation of a MEPPM symbol from 3 BIBD codewords ($N = 3$). In this example, codewords C_1, C_3 and C_6 of a $(11, 4, 1)$-BIBD code are added to create a symbol with length 11 and weight 12.

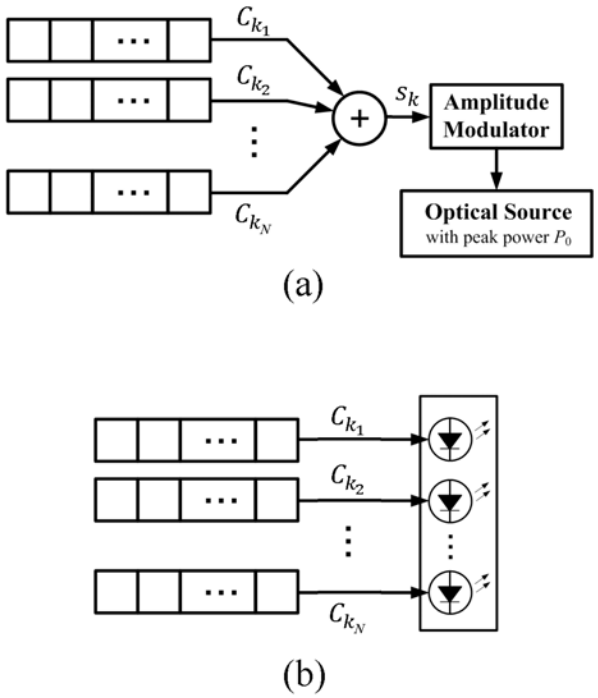


Fig. 2. Transmitter structure and symbol generation using N shift registers and using (a) a multilevel optical source such as laser, (b) an LED-array.

Since the BIBD code used to generate the multilevel symbols is assumed to be cyclic, the symbol generator circuit at the transmitter can be implemented using N shift registers in N branches, as depicted in Fig. 2. In the general case, the number of branches, N, can be different from the number of levels, L. The optical source in the transmitter can be either a laser or an LED-array. Therefore, there can be two structures for the transmitter. In the first structure, as shown in Fig. 2-(a), each shift register generates one BIBD codeword, and then the outputs of these N branches are added to generate the corresponding L-level symbol. The symbol generated is applied to an external amplitude modulator, which modulates the output power of the optical source. Lasers used as transmitters of FSO systems are peak power limited sources, and we assume the output optical power can be modulated between 0 and P_0. The number of power levels is flexible. For symbol S_k, the output power of the source in time-slot i is $s_{ki}P_0/(L-1)$.

An LED-array is the other option for an optical source used in FSO links for which accurate pointing is less critical. Ultraviolet (UV) communications [10] and indoor FSO systems [11] are two emerging technologies that can use LED-arrays as optical sources at the transmitter. In an LED-array, each LED can be turned on and off independently, and hence, the whole array can be considered as a multilevel source. Thus, it can be used directly as the optical source in Fig. 2-(a). Alternatively, the transmitter using an LED-array can be implemented as in Fig. 2-(b), in which each codeword is directly sent to a subset LEDs in the array, and hence, it is simpler than the structure in Fig. 2-(a). The array size determines the maximum number of levels, and $L-1$ should be a divisor of the array size.

In MEPPM, each set of N BIBD codewords determines

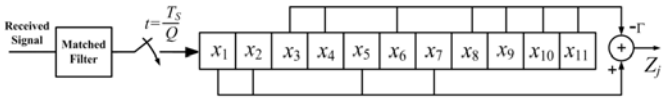


Fig. 3. Receiver for the MEPPM code shown in Fig. 1. T_s is the symbol period.

one symbol. Thus, as in EPPM, the front-end of the optimal receiver, assuming an additive Gaussian noise, can be implemented using a shift register with length Q [8], as shown in Fig. 3. In this figure, Γ is $\frac{\lambda}{K-\lambda}$. The receiver generates Q variables in each symbol period at the output of the differential circuit by circulating $X = \{x_1, x_2, \ldots, x_Q\}$, the received data stored in the shift register. The combination of the shift register and the differential circuit generates the decision statistic $z_j = \langle X, C_j\rangle - \Gamma\langle X, \overline{C}_j\rangle$, for $j = 1, 2, \ldots, Q$, where $\langle X, Y\rangle$ denotes the dot product of the vectors X and Y. Hence, the z_j's form a sufficient statistic for detection.

Due to the fixed cross-correlation property of the BIBD codewords, assuming that C_ℓ is transmitted, its contribution in the expected value of z_ℓ is $E\{z_\ell\} = \frac{\mathcal{E}}{L-1}K$, and in z_j, $j \neq \ell$, is $E\{z_j\} = 0$ [12], where $\mathcal{E}$ is the received energy in one time-slot for an unmodulated transmitted signal with peak power P_0.

Depending on whether the codewords used in the generation of the symbols must be distinct or not, MEPPM can be categorized into two types, discussed below.

A. Type I Multilevel EPPM

For this scenario, the N branches generate distinct codewords, and each codeword is used at most once in the generation of each symbol, i.e., $k_n \neq k_m$ for $\forall n \neq m$. Hence, the total number of symbols for type I MEPPM with N branches is $\binom{Q}{N}$. This constellation size is maximized for $N = Q/2$.

For this case, the energy of the symbol S_k is

$$|S_k|^2 = \Big|\sum_{n=1}^{N} C_{k_n}\Big|^2 = \sum_{n=1}^{N}|C_{k_n}|^2 + \sum_{n=1}^{N}\sum_{\substack{m=1\\ m\neq n}}^{N}\langle C_{k_n}, C_{k_m}\rangle, \tag{4}$$

which, using (1), becomes $|S_k|^2 = NK + N(N-1)\lambda$, for $\forall k$. Hence, all symbols have equal energy in type I MEPPM. For the receiver in Fig. 3, when symbol k is transmitted, we get $E\{z_j\} = \frac{\mathcal{E}}{L-1}K$ for $j \in \{k_1, k_2, \ldots, k_N\}$, and $E\{z_j\} = 0$ for $j \notin \{k_1, k_2, \ldots, k_N\}$. Thus, by finding the N largest z_j's we make an optimal decision on the received symbol. This detector does not require any threshold or energy compensation to make a decision.

In a (Q, K, λ)-BIBD code, the number of codewords that have "1" in a specific position is K. Therefore, for symbols composed of N different codewords, each element is less than or equal to K, i.e. $s_{ki} \leq K$ for $\forall k, i$. Hence, for type I, we have

$$L - 1 \leq \min\{N, K\}. \tag{5}$$

For $N \geq K$, which is typical, we have $L = K + 1$.

For a Gaussian additive noise channel, the symbol error probability is a function of the Euclidean distance between the symbols. Since the Hamming distance between the codewords of a (Q, K, λ)-BIBD code is $2(K - \lambda)$, the minimum Euclidean distance between the symbols of type I MEPPM is

$$d^E_{\min} = \frac{\mathcal{E}}{K}2(K - \lambda), \tag{6}$$

which, using (2), becomes

$$d^E_{\min} = 2\mathcal{E}(1 - \frac{K-1}{Q-1}). \tag{7}$$

This distance takes its maximum value for $K = 1$, which corresponds to using PPM constituent codewords. This means that the minimum error probability is achieved when the generating codewords are the symbols of the PPM scheme. For this case, type I MEPPM reduces to multipulse PPM (MPPM). When spectral-efficiency is important, the $Q = 2K + 1$ case is used since the complements of the codewords can also be included as codewords, but when power-efficiency is important, MPPM is preferred over type I MEPPM.

B. Type II Multilevel EPPM

In this case, different branches are allowed to have the same codewords, i.e., one codeword can be used more than once in the generation of each symbol. To calculate the constellation size, let n_k be the number of branches that have codeword C_k, where $0 \leq n_k \leq N$, then we have

$$\sum_{k=1}^{Q} n_k = N. \tag{8}$$

The energy of the symbol S_k for this type is

$$|S_k|^2 = \Big|\sum_{k=1}^{Q} n_k C_k\Big|^2 = \sum_{k=1}^{Q} n_k^2|C_k|^2 + \sum_{k=1}^{Q}\sum_{\substack{\ell=1\\ \ell\neq k}}^{Q} n_k n_\ell\langle C_k, C_\ell\rangle. \tag{9}$$

Using (1) and (8), we get

$$|S_k|^2 = (K - \lambda)\sum_{k=1}^{Q} n_k^2 + \lambda N^2. \tag{10}$$

As one can see, for type II MEPPM, the symbols do not have equal energies, and therefore, we need an energy compensator to make an optimal decision. For this type, the outputs of the receiver in Fig. 3 are $E\{z_j\} = \frac{\mathcal{E}}{L-1}n_j K$. The optimal detector can be implemented as

$$\max_{n_1, n_2, \ldots, n_Q} \sum_{k=1}^{Q} n_k\langle X, C_k\rangle - (K - \lambda)\Big(\frac{\mathcal{E}}{L-1}\Big)^2\sum_{k=1}^{Q} n_k^2. \tag{11}$$

Using the definition of z_k, the detector becomes

$$\max_{n_1, n_2, \ldots, n_Q} \sum_{k=1}^{Q}\Big(z_k - \mathcal{E}\frac{K}{L-1}n_k\Big)^2 \tag{12}$$

We can use an iterative decoder to find the optimal n_j's. In order to make an optimal decision, we define $w_j^{[m]}$ as the hypothesized n_j at iteration m, with initial value of $w_j^{[0]} = 0$. In each iteration, we update the weights as follows

$$w_j^{[m+1]} = \begin{cases} w_j^{[m]} + 1 & j = \arg \max\limits_{1 \le k \le Q} \left\{ z_k - w_k^{[m]} \mathcal{E}_{\frac{K}{L-1}} \right\}, \\ w_j^{[m]} & \text{otherwise.} \end{cases} \tag{13}$$

At step $m = N$, we set $n_j = w_j^{[m]}$. The most likely symbol sent uses n_k copies of C_k, $k = 1, 2, \ldots, Q$, assuming an additive white Gaussian noise (AWGN) channel.

The constellation size is equal to the number of solutions of (8), which is equal to $\binom{Q+N}{N}$. As can be seen, the constellation size for type II is larger than that of the type I, leading to a more spectrally efficient design. In contrast, it requires a more complicated receiver compared to type I.

We define M_ℓ as the number of symbols generated from exactly ℓ distinct codewords, which is equal to the number of integer solutions of

$$n_{k_1} + n_{k_2} + \cdots + n_{k_\ell} = N, \tag{14}$$

where $k_j \in \{1, 2, \ldots, Q\}$ for $j = 1, 2, \ldots, \ell$. The number of solutions to (14) is

$$M_\ell = \binom{Q}{\ell} \binom{N-1}{\ell-1}. \tag{15}$$

For type II MEPPM, the number of levels, L, is $N + 1$, independent from K. The minimum Euclidean distance for this case is

$$d_{\min}^E = 2 \frac{\mathcal{E}}{N} K \left(\frac{Q-K}{Q-1} \right). \tag{16}$$

As this discussed in [8], the optimum parameters to maximize $d_{\min}^E$ in (16) are $Q = 2K + 1$ and $K = 2\lambda + 1$.

C. Multilevel Augmented EPPM

For a BIBD code with $Q = 2K + 1$ and $K = 2\lambda + 1$, the Hamming distance between $\overline{C}_j$, the complement of C_j, and C_i is [8]

$$d(\overline{C_j}, C_i) = \begin{cases} Q & ; i = j, \\ 2\lambda + 1 & ; i \neq j. \end{cases}$$

Thus, the complements of codewords can also be included as symbols in EPPM with only a minor penalty on the minimum distance. The new scheme that is obtained by including the complements of codewords is called augmented EPPM (AEPPM) in [8]. Similarly, we can increase the constellation size using these complements in MEPPM. To do this, in Fig. 2, we first choose N codewords out of Q, and then in each branch we choose between the codeword and its complement. We call this scheme multilevel AEPPM (MAEPPM). In this way the constellation size for type I can be increased to $2^N \binom{Q}{N}$. For type II MAEPPM, using this approach the number of symbol generated from ℓ distinct codewords can be increased from M_ℓ to $2^\ell M_\ell$. So, the total number of symbols for type II MAEPPM is equal to

$$M = \sum_{\ell=1}^{N} 2^\ell \binom{Q}{\ell} \binom{N-1}{\ell-1} = P_N^{(Q-N,-1)}(3), \tag{17}$$

where $P_n^{(\alpha,\beta)}(x)$ is the Jacobi polynomial [13].

For MAEPPM the same receiver as Fig. 3 is used, and a similar decoding is applied to detect the symbol sent, except that, instead of the set $\{z_1, z_2, \ldots, z_Q\}$, we form the set $\{z_1, z_2, \ldots, z_Q, -z_1, -z_2, \ldots, -z_Q\}$ [8], and make a decision using this set.

III. Error Performance and Spectral-Efficiency

In this section we obtain expressions for the symbol error probability for the modulation schemes described in Section II. We use the resulting expressions to derive to derive the spectral-efficiency of the various schemes. We assume an additive white Gaussian noise channel with power spectral density $N_0/2$, as appropriate for thermal or background noise limited FSO systems. We model the effect of this noise by adding a Gaussian random variable with variance $\Delta f N_0$ to the decision statistic z_j, $j = 1, 2, \ldots, Q$, where Δf is the receiver bandwidth. Therefore, the optimum maximum likelihood (ML) decision rule reduces to the minimum distance criterion. For type I, since the energies of the symbols are the same, the performance of the correlation receiver in Fig. 3 is optimal. The union bound on the symbol error probability for an M-ary modulation can be expressed as [14, p. 334]

$$\mathrm{P}_s^{(U)} = \frac{1}{2M} \sum_{i=1}^{M} \sum_{\substack{j=1 \\ i \neq j}}^{M} \mathrm{erfc}\left(\sqrt{\frac{d_{ij}^H \gamma}{2(L-1)} \frac{\log_2 M}{Q}} \right). \tag{18}$$

where d_{ij}^H is the Hamming distance between symbols i and j. For an FSO system with bit-rate R_b, received peak optical power P_r (unmodulated) and photodetector responsivity ρ, we define the peak SNR as $\gamma = \frac{\rho^2 P_r^2}{N_0 R_b}$. For high SNRs, the smallest Hamming distance between symbols, $d_{\min}^H$, limits P_s, so (18) is approximated by

$$\mathrm{P}_s^{(U)} \approx \frac{M'}{2M} \mathrm{erfc}\left(\sqrt{\frac{d_{\min}^H \gamma}{2(L-1)} \frac{\log_2 M}{Q}} \right), \tag{19}$$

where M' is the number of symbol pairs with Hamming distance $d_{\min}^H$.

For type I MEPPM, we have $M = \binom{Q}{N}$ and, therefore, its spectral-efficiency is

$$\eta_{1,\text{MEPPM}} = \frac{\log_2 \binom{Q}{N}}{Q}. \tag{20}$$

The smallest Hamming distance between symbols is $d_{\min}^H = 2(K - \lambda)$ and $M' = \frac{N(Q-N)}{2} \binom{Q}{N}$. MPPM is a special case with $K = 1$ and $\lambda = 0$.

For type II MEPPM, the constellation size is $M = \binom{Q+N}{N}$, and hence, we have

$$\eta_{2,\text{MEPPM}} = \frac{\log_2 \binom{Q+N}{N}}{Q}. \tag{21}$$

For this type, $d^H_{\min} = 2(K-\lambda)$ and, for a symbol composed of ℓ distinct codewords, the number of pairs of symbols with Hamming distance $2(K-\lambda)$ is $\ell(Q-\ell)$. Hence, the total number of symbol pairs with distance $2(K-\lambda)$ is

$$M' = \frac{1}{2}\sum_{\ell=1}^{N} \ell(Q-\ell)M_\ell = \frac{Q(Q-1)}{2}\binom{Q+N-3}{N-1}. \quad (22)$$

For type I and type II MAEPPM, the minimum Hamming distance decreases to $d^H_{\min} = 2\lambda + 1$, and the spectral-efficiencies are

$$\eta_{1,\text{MAEPPM}} = \frac{N + \log_2 \binom{Q}{N}}{Q}, \quad (23)$$

and

$$\eta_{2,\text{MAEPPM}} = \frac{\log_2 P_N^{(Q-N,-1)}(3)}{Q}, \quad (24)$$

respectively.

To calculate the BER, we denote the assigned $(\log_2 M)$-bit binary sequence to symbol k by $\boldsymbol{b}_k$. When the transmitted symbol k is estimated incorrectly as symbol k', $d(\boldsymbol{b}_k, \boldsymbol{b}_{k'})$ bits are decoded incorrectly. Hence, for an M-ary modulation scheme, an upper bound on the BER is given by [14]

$$\mathrm{P}_b^{(U)} = \frac{1}{2M}\sum_{k=1}^{M}\sum_{\substack{k'=1\\k'\neq k}}^{M} \operatorname{erfc}\left(\sqrt{\frac{d^H_{kk'}\gamma}{2(L-1)}\frac{\log_2 M}{Q}}\right)\frac{d(\boldsymbol{b}_k,\boldsymbol{b}_{k'})}{\log_2 M}. \quad (25)$$

For all proposed multilevel schemes, the optimum bit-symbol mapping is similar to MPPM, and is a difficult problem. Hence, in our work, we use a random bit-symbol mapping, for which the BER is $\mathrm{P}_s^{(U)}/2$.

IV. Numerical Results

In this section, numerical results are presented to compare the performance of MEPPM and MAEPPM with other schemes. We use Paley, projective geometry (PG) and twin prime power (TPP) difference sets [9] as BIBD code families in these results, as for these code families $Q = 2K+1$ and $K = 2\lambda + 1$.

Fig. 4 shows the spectral-efficiency from (20)-(24) versus the required peak SNR, γ, for a BER of 10^{-5}, for OOK, PAM, MPPM, type I and II MEPPM, and type I and type II MAEPPM from (19) and (25). Each point represents a scheme with different parameters. For all multilevel modulation schemes, $N = (Q-1)/2$ and Q is $7, 11, 19, 35, 67, 131$ and 263. MPPM, MEPPM and MAEPPM are able to achieve high spectral-efficiencies since their constellation sizes are large. From these plots, the spectral-efficiency is the same for MPPM and type I MEPPM, but MPPM requires a lower γ. Among all pulse-position based schemes type II MAEPPM is the most efficient modulation for spectrum usage. Type II MAEPPM is able to achieve 75% higher spectral-efficiency compared to MPPM with only a small SNR penalty.

The symbol error probability of PPM, EPPM, MPPM, MEPPM and MAEPPM are compared for a fixed bit-rate in Fig. 5 for an FSO link. For all these schemes $Q = 19$ and

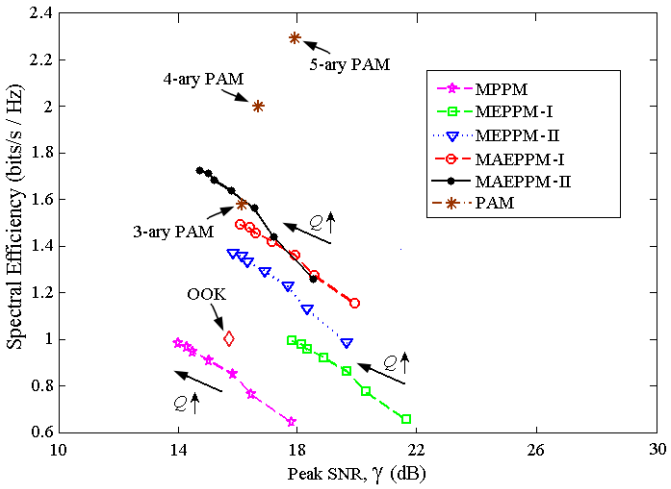


Fig. 4. Analytical spectral-efficiency and required γ for BER of 10^{-5}, for OOK, PAM, MPPM, type I and type II MEPPM, and type I and type II MAEPPM .

$N = 9$, and for MEPPM and MAEPPM a (19,9,4)-BIBD code is used. According to these results, EPPM has the best performance among all techniques.

To test the performance of our modulation scheme in a dispersive environment in the absence of an equalizer, the BER of on-off keying (OOK), PAM, EPPM and type II MAEPPM schemes are compared in Fig. 6 for a dispersive FSO link. A practical example of a dispersive FSO link is non-line of sight ultraviolet (NLOS-UV) communications [15]. For this FSO link, the channel impulse response is assumed to be Gaussian with broadening factor σ, i.e. $h(t) = \frac{1}{\sqrt{2\pi}\sigma}\exp(-t^2/2\sigma^2)$. Here we assume γ is 16 dB. For EPPM and type II MAEPPM, a BIBD code with $Q = 19$, $K = 9$ and $\lambda = 4$ is used. The BERs are plotted versus the normalized broadening factor, σR_b, where R_b is the bit-rate. The transmitted signal is assumed to have a non-return-to-zero rectangular pulse

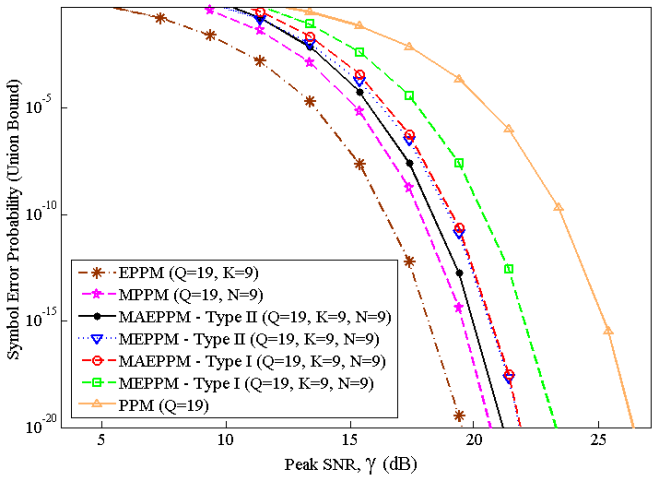


Fig. 5. Union bound on symbol error probability of an FSO link versus γ for PPM, EPPM, MPPM ($N = 9$), type I and type II MEPPM ($N = 9$), and type I and type II MAEPPM ($N = 9$). For all these schemes $Q = 19$.

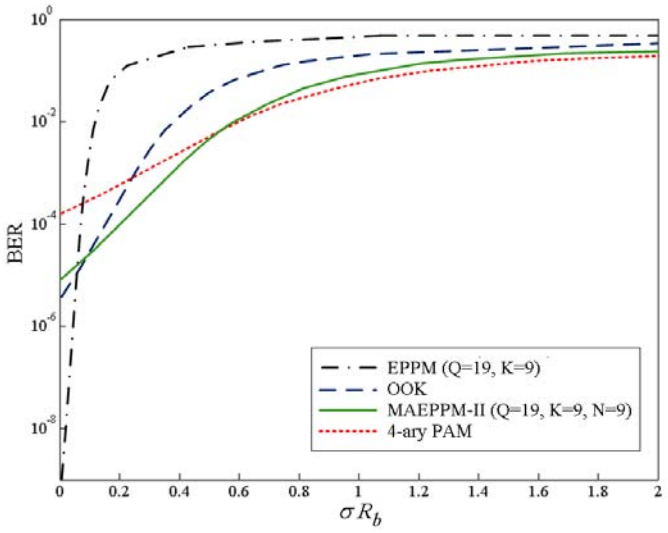


Fig. 6. Simulated BER vs. normalized broadening factor for a FSO link for OOK, EPPM, type I MAEPPM and 4-ary PAM.

shape, and the received pulse is obtained by convolving the transmitted signal with the channel impulse response. By increasing σR_b, the ISI effect becomes the dominant limit, and, therefore, schemes with higher spectral-efficiencies perform better. Although EPPM has the lowest BER for non-dispersive channels, it is the most vulnerable scheme to ISI since it has the lowest spectral-efficiency. On the other hand, while 4-ary PAM has the best performance in high dispersive channels, because of its low BER at $\sigma = 0$, it is not the best technique for low dispersive channels. Type II MAEPPM has the best performance for medium dispersion cases, and suffers only a small performance penalty compared to 4-PAM in high dispersion cases.

V. Conclusion

In this paper, novel modulation schemes called multilevel expurgated PPM are proposed. The symbols are constructed by combining several BIBD codewords. Indeed, the symbols of these schemes can be considered as a subset of combined PPM-PAM symbols. Because of the large constellation sizes that can be achieved, the proposed schemes are more spectrally efficient than MPPM, PPM and EPPM. Simple transmitter and receiver structures using shift registers are presented. MEPPM is divided into two types, based on the variety of the codewords that can be considered in the generation of the symbols. It is shown that by adding the complements of the BIBD codewords, a larger constellation size can be attained for the same transmitter/receiver structures. Analytical symbol error probabilities and spectral-efficiencies are calculated, and numerical results are presented to compare the performance of the proposed schemes with other modulation techniques. The application of MEPPM and MAEPPM in dispersive FSO channels is also discussed, and their performances are compared with OOK and PAM. The proposed schemes are shown to outperform existing techniques over dispersive channels.

VI. Acknowledgment

This research was funded by the National Science Foundation (NSF) under grant number ECCS-0901682.

References

[1] K. Kiasaleh, "Performance of APD-based, PPM free-space optical communication systems in atmospheric turbulence," *IEEE Trans. Commun.*, vol. 53, no. 9, pp. 1455–1461, 2005.

[2] S. G. Wilson, M. Brandt-Pearce, Q. Cao, and J. H. Leveque, "Free-space optical MIMO transmission with Q-ary PPM," *IEEE Trans. Commun.*, vol. 53, no. 8, pp. 1402–1412, 2005.

[3] Z. Xu, "Approximate performance analysis of wireless ultraviolet links," *IEEE ICASSP Conf.*, 2007.

[4] H. Sugiyama and K. Nosu, "MPPM: a method for improving the band-utilization efficiency in optical PPM," *J. Lightw. Tech.*, vol. 7, no. 3, pp. 465–472, 1989.

[5] H. Zhang, W. Li, and T. Gulliver, "Pulse position amplitude modulation for time-hopping multiple-access uwb communications," *IEEE Trans. Commun.*, vol. 53, no. 8, pp. 1269–1273, 2005.

[6] Y. Zeng, R. Green, and M. Leeson, "Multiple pulse amplitude and position modulation for the optical wireless channel," *International Conference on Transparent Optical Networks (ICTON)*, pp. 193–196, Aug. 2008.

[7] M. Herceg, D. Zagar, and D. Galic, "Multi pulse position amplitude modulation for ultra-high speed time-hopping UWB communication systems over AWGN channel," *International Symposium on Communications, Control and Signal Processing (ISCCSP)*, May 2010.

[8] M. Noshad and M. Brandt-Pearce, "Expurgated PPM using balanced incomplete block designs," *IEEE Commun. Lett.*, vol. 16, no. 7, pp. 968–971, 2012.

[9] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs, 2nd Ed.* Chapman and Hall-CRC, 2007.

[10] Z. Xu and B. Sadler, "Ultraviolet communications: Potential and state-of-the-art," *IEEE Commun. Magazine*, vol. 46, no. 5, 2008.

[11] L. Zeng, D. O'Brien, H. Minh, G. Faulkner, K. Lee, D. Jung, Y. Oh, and E. T. Won, "High data rate multiple input multiple output (MIMO) optical wireless communications using white LED lighting," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1654–1662, 2009.

[12] M. Noshad and K. Jamshidi, "Code family for modified spectral-amplitude-coding OCDMA systems and performance analysis," *J. Opt. Commun. Netw.*, vol. 2, no. 6, pp. 344–354, 2010.

[13] D. Zwillinger, *CRC Standard Mathematical Tables and Formulae, 32nd Ed.* Taylor and Francis, 2011.

[14] S. S. Haykin, *Communication Systems, 4th Ed.* John Willey & Sons, 2001.

[15] M. Noshad and M. Brandt-Pearce, "NLOS UV communication systems using spectral amplitude coding," *Proceding of IEEE Global communications conference (GLOBECOM)*, pp. 843–848, Houston, TX, Dec. 2011.

deStress: Mobile and Remote Stress Monitoring, Alleviation, and Management Platform

Jin Zhang[†], Hao Tang[‡], Dawei Chen[†] and Qian Zhang[†]
[†] Hong Kong University of Science and Technology
{jinzh, dwchen, qianzh}@cse.ust.hk
[‡] Shenzhen New Element Medical Equipment Technology Development Co.
tanghao@szxys.cn

***Abstract*—Excessive stress may lead to health problems like headache, trouble sleeping, depression and chronic diseases such as cardiovascular and cerebrovascular diseases. In this paper we present deStress, the mobile and remote stress monitoring, alleviation and management system, whose features are: firstly it is wearable and inexpensive, which uses only one wearable stress monitor sensor and a mobile phone-based application (Android OS) to monitor stress. Secondly, deStress quantitatively assesses the user's stress level continuously, not just classifies the users into stressed or non-stressed state. Thirdly, deStress provides a system for stress monitoring and management, through which the stress data could be recorded, analyzed and shared with medical professionals. Last but not least, a novel adaptive respiration-based bio-feedback approach is implemented to alleviate stress. To the best of our knowledge, deStress is the first telehealth system dedicated to mobile and remote stress monitoring, alleviation and management. Extensive experiment are conducted in 30 persons to demonstrate the feasibility and effectiveness of deStress, and the result shows that the stress level assessment of deStress correctly indicates the mental states of the users, and under the guidance of deStress the users could alleviate their stress level dramatically.**

***Index Terms*—Stress Monitoring, Stress Alleviation, Stress Management, Remote Health Monitoring**

I. Introduction

In everyday life, stress could be a positive factor for people to increase excitement and improve performance of tasks [1] [2]. However, excessive stress may lead to health problems like headache, trouble sleeping, depression and chronic diseases such as cardiovascular and cerebrovascular diseases [3]–[5]. Existing studies on animal and human have shown that stress is also an important factor that leads to psychological or behavioral problems like rage and anxiety [6]–[9].

Accurate stress monitoring and effective stress alleviation systems are supposed to be great helpful for people to keep healthy. Although extensive research has been conducted to understand the relations between psychological changes and physiological changes [10] [11], most of the conclusions are subjective and qualitative. Therefore, a quantitative and objective approach to monitor and alleviate stress in real-time will be of significant meaning.

Majority of the existing stress monitoring systems rely on self-report which may be unreliable and miss stress episodes [12]. Although there are laboratory-based systems that automatically detect the mental emotions, they suffer from portability, which require a large number of sensors and extensive human involvement, thus cannot be used to monitor the stress in everyday life by ordinary users [13]–[16]. There are also portable stress monitoring systems, but they require multiple sensors and complex algorithms for stress assessment, which make the system computationally expensive, energy consuming and uncomfortable to wear in everyday life for long time evaluation [17] [18]. Among all the above stress monitoring systems, the authors tried to classify the subject into stressed and non-stressed states, but practical applications require more precise stress assessment such as quantitative stress level assessment. Moreover, the absence of a remote wireless system makes the existing portable systems unable to provide real-time health intervention from medical staffs to users.

When the stress level of a user is assessed to be high, stress alleviation is of great helpful. It is well known that taking physical activities could be of great help to alleviate mental stress, among which controlled breath has been proved to be a simple and effective approach [19]. A common challenge of all the stress alleviation approaches is that they cannot assess the benefit to the subject in real-time because they lack of a real-time feedback and assessment scheme.

Motivated by these challenges, in this paper we propose deStress, a mobile & remote stress monitoring, alleviation and management system, which could not only measure stress quantitatively in real-time, but also utilize bio-feedback approaches to guide the users to alleviate stress level using graphic user interface (GUI) based on the stress monitoring result. Our system has several novelties and advantages. Firstly, it is inexpensive. The client side of our system is a mobile phone-based application (currently on Android OS), which uses only one wearable stress monitor sensor to collect biomedical signal. Secondly, deStress quantitatively assesses the user's stress level in a continuous range, not just classifies the users into two states. Thirdly, deStress provides a system for stress monitoring and management, through which the stress data could be recorded, analyzed and shared by medical professionals if needed. Last but not least, a novel adaptive respiration-based bio-feedback approach is implemented to alleviate stress.

To the best of our knowledge, deStress is the first telehealth system dedicated to mobile and remote stress monitoring,

alleviation and management. The contributions of the paper are: we design and implement deStress, specifically we

1) design and implement the stress monitoring sensor which could quantitatively assess the holder's stress level and as small as a wrist-watch.
2) design and implement an accurate stress monitoring and an effective stress alleviation algorithm.
3) conduct experiments in 30 persons to demonstrate the feasibility and effectiveness of our system. The experimental results show that our stress level assessment correctly indicates the mental states of the users, and under the guidance of deStress, the users could alleviate their stress level dramatically.

The rest of the paper is organized as follows. First the system design is presented in Section II. Then we introduce our algorithm for stress monitoring and alleviation in Section III. After that we evaluate deStress in Section IV. The related work is introduced in Section V. Finally we conclude the paper in Section VI.

II. System Design

A. Requirements and Challenges

To meet the strict medical requirements of the hospital, clinic and scientific community researching on human stress and related disciplines, we need to pay close attention to the following requirements and challenges.

1) Terminal Versatility: Rather than a single product, the system proposed in this paper is more like an integration solution. Thus, it is important to increase the system flexibility and reduce the customer's cost. For instance, customers may want to use their existing mobile phones instead of purchasing a new handset. To solve it, the software run on mobile phones should support most mainstream mobile operation systems. Moreover, the stress monitor should be able to communicate with mobile phones which may use different protocols of short distance communication in personal area networks (PANs). All these factors give rise to the challenges of terminal versatility.

2) Data Transmission and Storage: There are two types of data transmission: the channel between stress monitor and terminal, and the channel between central server and terminal. For each of them, we need to consider both transmission rate and reliability. Terminals should also have enough storage capacity to store the sensor data of one user when it used as an off-line stress monitoring device or when the network condition is not good. Also, in the case for multiple users the large storage capacity is necessary, e.g., the scenario of school application when one device is used by the whole class. Regarding the central server storage, when deStress is used in large scale, the sensor data and user data will be massive, therefore the cloud-based storage need to be considered.

3) Sensor Data Quality and Validation: Unlike normal health monitoring device in hospital, we are designing a remote health monitoring system where there is no medical staff or specialist who provides on-site test guidance and validation of data effectiveness. Therefore, the system need to pay attention to manage and validate the remote physiological sensor data intelligently, for instance, the detection of human speaking, movement, data missing, sensor detachment, etc.

4) Wearability and Battery Life: To maximize the accuracy and effectiveness of stress evaluation, and better demonstrate the mobility and portability of the system, it should minimize the burden or uncomfortableness caused by the wearable sensor. Also, to make stress monitor convenient to use, the battery capacity should be large enough to guarantee long time use and save the trouble of frequent battery replacement and recharging. Tradeoffs have to be made among the sensor accuracy, wearability, weight and cost as well. Moreover, our solution that using only one single physiological sensor for both stress evaluation and adjustment, rather than in most cases where an additional respiratory sensor is used for respiratory signal extraction, leads to great challenges.

5) Algorithm Efficiency and Computational Inexpensiveness: Since this is a smart phone-based application, the software and algorithm should be implemented with low computation cost and high performance. The high performance includes the high quality of interaction and user experience, e.g., low latency time. Meanwhile, the low computation cost is essential to reduce the energy consumption and increase the battery life.

B. Architecture

To meet the requirements and solve the challenges mentioned above, we use only one wearable physiological sensor to increase the user comfortableness, build a cloud system for the stress data management, design a efficient stress monitoring algorithm to quickly monitor the stress level and increase the battery life, and implement a GUI on smart phone platforms to improve the user experiences.

The whole system has three main components: wearable stress monitor, terminal (smart-phones, pads or tablets) and the back cloud server (web-based telehealth system). These three components are physically disconnected and communicated with each other using wireless communication. The architecture is show in Figure 1.

The server functions as a central system which provides basic services for the entire remote stress management system, such as user and device management, data security and storage, information analysis and processing. The terminal here refers to the health mobile phone or tablet, on which the key algorithm for stress evaluation and alleviation was run. It communicates with stress monitor and central server via Bluetooth and 3G or Wi-Fi respectively. Currently, we implemented our algorithm on mobile phones. The stress monitor continuously collects physiological data, communicates with the terminal via Bluetooth, and transmits collected physiological data to the terminal. Since the discussion of the design and functionality of the server is beyond the scope of this paper, hereafter we will focus on the stress monitor, and the GUI in the terminal and web-site.

1) Stress Monitor: The primary challenge for the design of stress monitor is to achieve satisfactory accuracy and stable

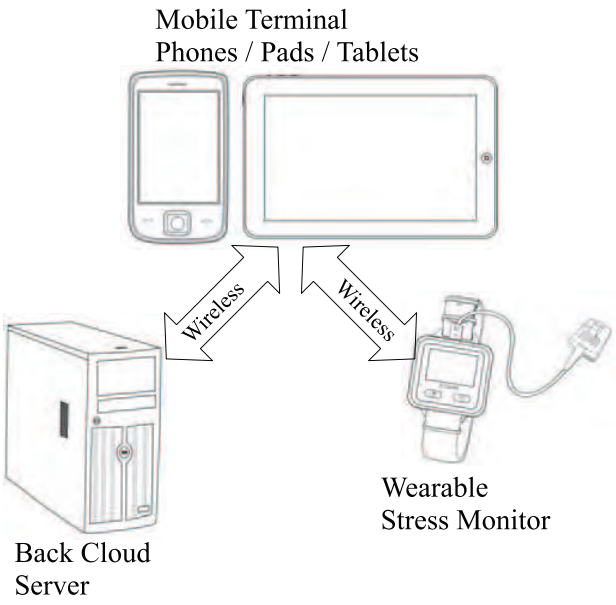


Fig. 1. System Architecture.

Fig. 2. Stress monitor of deStress.

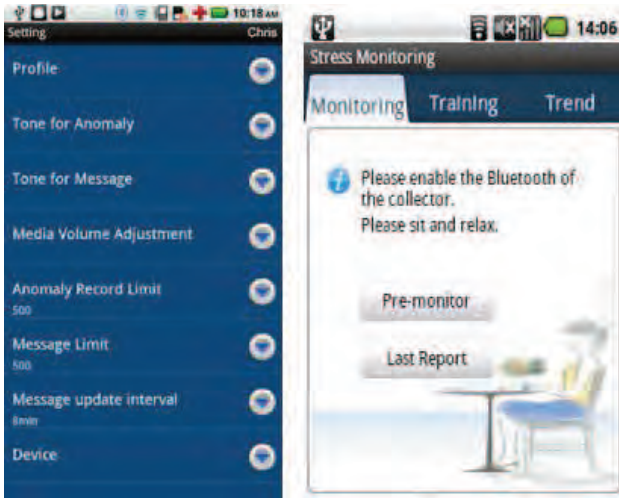


Fig. 3. GUI at the terminal side.

connectivity to mobile devices, while at the same time maximizing its portability and wearability. Moreover, the energy consumption also needs to be optimized.

To address above challenges, as shown in Figure 2, the exterior of the stress monitor is designed as a wristwatch style with a rubber finger-cot for collecting PPG signals affixed. Two sensors are applied for our stress monitor, one is a pulse wave sensor (pulsometer), which monitors photoplethysmograph (PPG) signal, the other is a tri-axial accelerometer, which measures the acceleration signal. The hardware circuits is composed of the following modules: PPG sensor module, tri-axial accelerometer module, MCU module, Bluetooth module, display module, battery management module and peripheral components.

The MCU is the core module of the stress monitor, it controls the work and communications of other modules, uses interrupt to digitize and sample data from pulsometer and tri-axial accelerometer sensors. An ARM-based ARM_Cortex-M3 MCU is applied, with the maximum frequency of 72 MHz.

For the real-time stress monitoring and alleviation purposes, we have tried different sensors and numerous research and tests have been conducted. Finally, we choose the pulsometer instead of Electrocardiography (ECG) for Heart rate variability (HRV) analysis and a tri-axial accelerometer for physical activity detection.

Pulsometer, is a blood volume pulse detection sensor, housed in a small finger worn package, to measure heart rate and blood volume changes, and heart rate variability.

The stress monitor uses Bluetooth module (currently we use Bluetooth 2.1 protocol) for wireless transmission. It has a built-in 2.4G Bluetooth antenna RF with a working distance of 10 meters.

2) Graphical User Interface: The GUI is implemented at both terminal side and on the web. At terminal side, the GUI is designed to enable the users to view the stress monitoring result, configure the terminal, and guide the users to alleviate stress. The GUI on the web-site is designed to manage the medical data collected from the terminals.

The GUI is showed in Figure 3 and 4.

III. Algorithm Design

A. Background of Stress Monitoring and Alleviation

In this subsection we will give a brief introduction to the theory of stress monitoring and alleviation.

In quiet state the psychology stress could be detected via measuring the heart rate variability. HRV is the time difference between each heartbeat (R-wave), i.e. the beat-to-beat variability. Each R-wave represents a contraction of the heart and corresponds to the pulse.

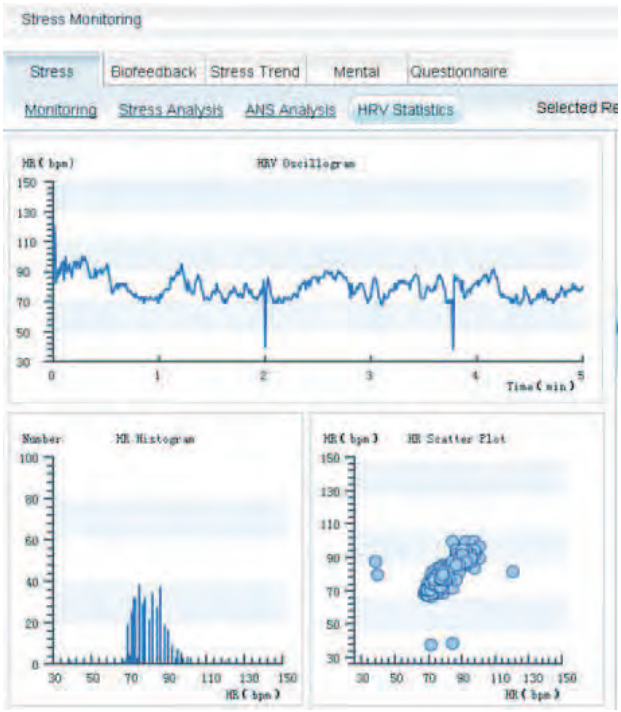


Fig. 4. GUI on the web-site.

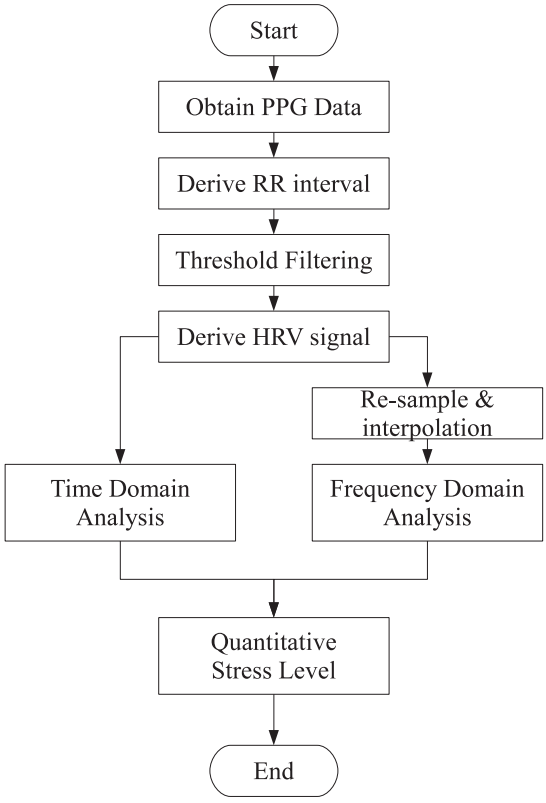


Fig. 5. Stress Monitoring Algorithm

The human organism is under the continuous control of the autonomic nervous system (ANS), which can be divided into two components: sympathetic nervous system (SNS) and the parasympathetic nervous systems (PNS). It is generally acknowledged that HRV is affected by ANS activities. Specifically speaking, the SNS increases the heart rate and PNS on the contrary decreases the heart rate.

HRV is the direct result of the interaction between these two autonomic nervous systems. In healthy conditions, the heartbeat should vary from beat to beat under a balanced control of both the SNS and PNS. However, in some cases, the balance would be broken. For instance, when suffering chronic stress, the SNS will over-dominate ANS. Therefore we can analyze HRV to investigate the ANS function and the related mental stress conditions.

HRV could be obtained from the ECG data or the PPG signal. When a person is in quiet or slow moving status, the HRV obtained from ECG and PPG are similar. However, PPG sensor is more comfortable than ECG sensors for the users. Thus in this paper we use PPG signal instead of ECG.

To alleviate the stress, physical exercise is well accepted by the public to be effective. Among all the physical activities, controlled respiration is considered to be a simple (perhaps the simplest) yet effective approach. L. Bernardi *et. al.* [19] found out the relation between the controlled breathing and the mental stress. However the effects of respiration vary among different people, thus we need a feedback system to adaptively adjust the respiration parameters.

B. Stress Monitoring Algorithm

As we have introduced, we need to obtain the SNS and PNS component from the HRV data. PNS takes effects fast and is the high frequency (HF, 0.15-0.40Hz) component, while SNS take effects slowly thus dominates the low frequency (LF, 0.04-0.15Hz) component. Therefore SNS and PNS component can be analyzed at frequency domain. And the energy ratio of LF to HF is an important indicator of mental stress.

The challenge of the monitoring algorithm is that our stress monitoring system should give the analysis result fast (e.g. within 60 seconds) because it is the most important information to adaptively adjust the treatment in stress alleviation. However, the sooner comes out the result, the less data we could collect, which may lead to insufficient resolution of frequency domain analysis. To solve this problem, we also conduct time-domain analysis on the PPG data and jointly consider the time-domain and frequency domain analysis results.

The flow chart of the stress monitoring algorithm is shown in Figure 5.

C. Stress Alleviation Algorithm

In this work we choose controlled respiration as the stress alleviation approach as it is simple yet efficient. deStress will guide the users to perform the controlled respiration, and give suggestions of adjusting the respiration frequency according to the feedback.

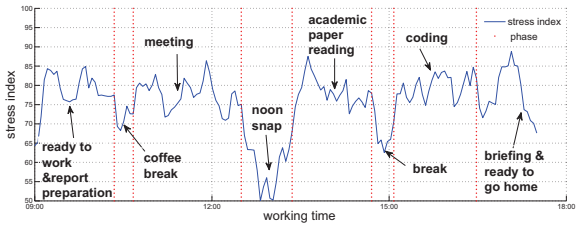


Fig. 6. Stress monitoring at day-time.

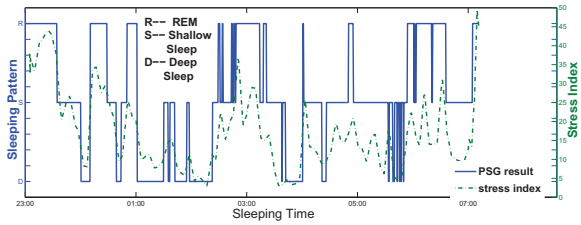


Fig. 7. Stress monitoring during sleep.

According to existing researches [19], 0.1 Hz is considered to be the optimal respiration frequency in general cases. Thus in this work we use 0.1 Hz as the initial respiration frequency if no prior knowledge is available.

0.1 Hz is not the optimal respiration frequency for every person. Thus, after the user performs the controlled respiration for a while, deStress will measure the stress level of the user and then rank the alleviation effect. According to the ranking, deStress will suggest the user to keep or adjust the respiration frequency.

IV. Performance Evaluation

The deStress system is evaluated via the real experiments carried out by 30 volunteers (customers). The age range was 26 ± 10 years, and body weight was 63 ± 10 kg, and none of subjects was taking medication.

To validate the system's precision of stress assessment and demonstrate the effectiveness of stress alleviation, we designed three experimental conditions and corresponding experiments were conducted on the above volunteers.

A. Baseline and Mental Stress Test

This experiment was designed to illustrate how the stress level varies during a workday given a office related background. It was conducted over a whole workday, and twice each individual.

The stress monitor is worn on the middle finger of left hand. Since all the volunteers are right-handed, it does not affect normal office work except typing with both hands. The data is collected in real-time via Bluetooth, and trigger the algorithm to calculate current stress level once a new data set of three minutes received. If the data quality score is below the threshold, we maintain the previous stress level. Self-report mechanism is also applied for collecting ground truth. In this case, self-reports prompt every 30 minutes, identical to ten times of stress assessment.

The experimental result is shown in Figure 6, from which we can see that the stress level is higher when working, and lower when rest.

B. Sleep Test

The motivation of this experiment is to investigate the relationship between mental stress level and different sleep pattern. It was conducted on 30 volunteers over two months, and they were given both our stress monitoring device and a sleep management product (ZEO[1], which provides sleep pattern analysis). Each individual was tested on two consecutive nights to address problems like unsuccessful data collection, as this was completely done at their own homes. Although guidance has been provided, some problems like sensor detachment, data missing when sleeping are inevitable to occur.

The signals of the entire night are divided into fragments of 5 minutes. Each fragment is analyzed independently and the corresponding stress level is computed, while ZEO gives the corresponding sleep pattern. Because the experiment data are collected simultaneously and divided into time window of the same length, a comparison between the stress levels and different sleep patterns are feasible.

The experimental result is shown in Figure 7. We could see that user's stress level is noticeable lower when in deep sleep, and much higher when in REM (rapid eye movement) sleep, which corresponds to the research on sleep patterns.

The experimental results of Figure 6 and 7 demonstrate the precision of our stress assessment index.

C. Stress Alleviation

This experiment was intended to study the effect of biofeedback method on the alleviation of mental stress level. Each one of the 30 volunteers was given a lab test lasting about 20 minutes. The participant was strictly asked to keep comfortable and quiet sitting posture without any talking or body movement. The test begins with a 5 minutes stress evaluation session followed by a 2-3 minutes rest period, and then a 5 minutes stress alleviation session followed with another 2-3 minutes rest period, and finally we test the participant with another stress evaluation session.

The experimental result is shown in Figure 8. We could see that the stress level drops dramatically after alleviation. From this we conclude that the respiration-based stress alleviation approach is effective to help the users to alleviation the stress under the guidance of deStress.

V. Related Work

The challenges of this work are mainly from stress monitoring category and stress alleviation category. In this section we will present the related work in both categories.

Nowadays the researchers measure the psychological state by measuring the physiological state. Ever since 1890 W. James *et. al.* raised the question about the relation between

[1]http://www.myzeo.com

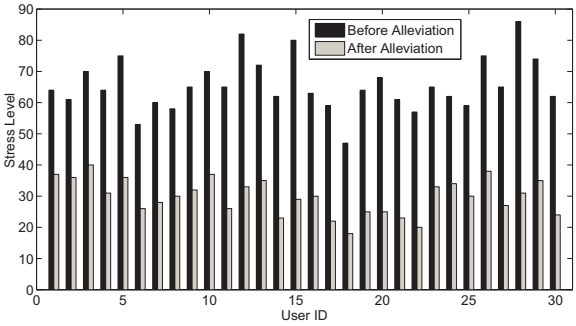


Fig. 8. Experimental result of stress alleviation.

physiology and psychology [11]. Over more than one hundred years several indicators have been found to be effective to infer or predict the stress, such as heart rate, HRV, blood pressure, RSA and so on, which is the theoretical foundation of the stress monitoring systems [10].

In recent years several portable stress monitoring systems are proposed to predict the psychological stress of in the natural environment. Compared with the laboratory-based systems, these systems need to handle the measurement noise generated in the everyday life such as speaking, walking, etc. K. Plarre *et. al.* used AutoSense wearable system to collect the ECG and respiratory inductive plethysmograph (RIP) data [18]. They trained and tested two models for continuous prediction of stress from physiological measurements from 21 subjects. A. Raij *et. al.* proposed mStress to monitor the stress via a Android phone based system [17]. mStress was evaluated in the natural environment of 23 subjects. In mStress, the time between capturing a sample from the participant and the making of an inference is, on average, 118 seconds, and the vast majority of this time (approximately 100 seconds) is spent in the Features Layer computing statistical features. The problems of these works are that they need to deploy multiple sensors on the subjects and rely on complex algorithms, which consumed lots of energy and made the users uncomfortable. Our system handles the problem by using only a PPG sensor and proposes an energy-efficient algorithm.

In stress alleviation category, L. Bernardi *et. al.* found out that the controlled breathing affected the HRV, and further affected psychological stress [19]. However in natural environment the effect of respiration activity is difficult to assess quantitatively, and the effects may vary among different subjects. Motivated by this, our system not only provide a stress monitoring system, but also provide a feedback algorithm to set the optimal personalized respiration parameters and adaptively adjust the target respiration frequency.

VI. Conclusion

In this paper we proposed deStress, the mobile and remote stress monitoring, alleviation, and management system. In this system we quantitatively assessed the user's stress level in a continuous range, and guided the users to alleviate the stress using a respiration-based approach. deStress was tested by 30 volunteers. To the best of our knowledge, deStress is the first telehealth system dedicated to mobile and remote stress monitoring, alleviation and management.

VII. Acknowledgement

This work is supported in part by Hong Kong RGC grants No. 623209, 622410, Huawei-HKUST joint lab, and National Natural Science Foundation of China with grant no. as 60933012, 61173156.

References

[1] J. Cacioppo and L. Tassinary, *Principles of psychophysiology: Physical, social, and inferential elements*. Cambridge University Press, 1990.
[2] H. Ursin and R. Murison, "Classification and description of stress," *Neuroendocrinology and psychiatric disorder*, pp. 123–132, 1984.
[3] M. Al'Absi and D. Arnett, "Adrenocortical responses to psychological stress and risk for hypertension," *Biomedicine & pharmacotherapy*, vol. 54, no. 5, pp. 234–244, 2000.
[4] G. Chrousos and P. Gold, "The concepts of stress and stress system disorders," *JAMA: the journal of the American Medical Association*, vol. 267, no. 9, pp. 1244–1252, 1992.
[5] B. McEWEN, "Protection and damage from acute and chronic stress: allostasis and allostatic overload and relevance to the pathophysiology of psychiatric disorders," *Annals of the New York Academy of Sciences*, vol. 1032, no. 1, pp. 1–7, 2004.
[6] J. Henry, "Stress, neuroendocrine patterns, and emotional response." 1990.
[7] M. al Absi, *Stress and addiction: Biological and psychological mechanisms*. Academic Pr, 2007.
[8] M. Enoch, "Pharmacogenomics of alcohol response and addiction," *American Journal of Pharmacogenomics*, vol. 3, no. 4, pp. 217–232, 2003.
[9] M. ENOCH, "Genetic and environmental influences on the development of alcoholism," *Annals of the New York Academy of Sciences*, vol. 1094, no. 1, pp. 193–201, 2006.
[10] J. Cacioppo and L. Tassinary, "Inferring psychological significance from physiological signals." *American Psychologist*, vol. 45, no. 1, p. 16, 1990.
[11] W. James, *The principles of psychology*. New York: Holt, 1890.
[12] F. Wilhelm and P. Grossman, "Emotions beyond the laboratory: Theoretical fundaments, study design, and analytic strategies for advanced ambulatory assessment," *Biological Psychology*, vol. 84, no. 3, pp. 552–569, 2010.
[13] J. Healey, L. Nachman, S. Subramanian, J. Shahabdeen, and M. Morris, "Out of the lab and into the fray: Towards modeling emotion in everyday life," *Pervasive Computing*, pp. 156–173, 2010.
[14] M. Myrtek and G. Brügner, "Perception of emotions in everyday life: studies with patients and normals," *Biological psychology*, vol. 42, no. 1, pp. 147–164, 1996.
[15] S. Kreibig, "Autonomic nervous system activity in emotion: A review," *Biological psychology*, vol. 84, no. 3, pp. 394–421, 2010.
[16] S. Kreibig, F. Wilhelm, W. Roth, and J. Gross, "Cardiovascular, electrodermal, and respiratory response patterns to fear-and sadness-inducing films," *Psychophysiology*, vol. 44, no. 5, pp. 787–806, 2007.
[17] A. Raij, P. Blitz, A. Ali, S. Fisk, B. French, S. Mitra, M. Nakajima, M. Nuyen, K. Plarre, M. Rahman *et al.*, "mstress: Supporting continuous collection of objective and subjective measures of psychosocial stress on mobile devices," *ACM Wireless Health 2010 San Diego, California USA*, 2010.
[18] K. Plarre, A. Raij, S. Hossain, A. Ali, M. Nakajima, M. Al'absi, E. Ertin, T. Kamarck, S. Kumar, M. Scott *et al.*, "Continuous inference of psychological stress from sensory measurements collected in the natural environment," in *Information Processing in Sensor Networks (IPSN), 2011 10th International Conference on*. IEEE, 2011, pp. 97–108.
[19] L. Bernardi, J. Wdowczyk-Szulc, C. Valenti, S. Castoldi, C. Passino, G. Spadacini, and P. Sleight, "Effects of controlled breathing, mental activity and mental stress with or without verbalization on heart rate variability," *Journal of the American College of Cardiology*, vol. 35, no. 6, pp. 1462–1469, 2000.

The measure of security in quantum cryptography

Marcin Niemiec and Andrzej R. Pach
Department of Telecommunications
AGH University of Science and Technology
Mickiewicza 30, 30-059 Krakow, Poland
Emails: {niemiec, pach}@kt.agh.edu.pl

***Abstract*—This paper describes a new concept of security measurement in quantum cryptography (QC). The most popular quantum key distribution protocol BB84 and the key distillation process are briefly introduced first. Next, a new concept of entropy of security in QC is proposed, and a unique measure of security is defined. Using this quantitative approach to security, it is possible to manage security and personalize services based on QC. Two different security levels are defined: the basic security level and the advanced security level. This differentiation of security enables us to choose the appropriate security level for specific end-users' requirements and needs. The last section presents the results of simulation experiments which verified the proposed solution.**

I. Introduction

Humankind's need for secret communication is at least as old as our civilization. We know that ancient societies had developed and used many methods of communicating secretly. Unfortunately, these imperfect solutions were simple to crack. Nowadays, there are entirely new methods of solving the security problem, utilizing the laws of physics to ensure that all eavesdroppers are uncovered. This concept, called quantum cryptography (QC), provides the highest security level, unrivalled by previous solutions.

The term security is an abstract concept which can cause serious problems during the measurement process. Usually we are able to determine if a given communication system is secure or not, although we cannot specify the level of security. For this reason, controlling system security is very difficult. This paper summarizes a part of dissertation [1]: it describes a new concept for defining the security of systems using QC in a quantitative way. This approach is crucial while striving to respect end-user requirements (such as security, cost, performance, etc.). Using this idea, end-users of a given QC system can select an appropriate security level.

II. Quantum cryptography

Cryptography is the main solution for ensuring data confidentiality. It transforms the message to make it unreadable to anyone except the appropriate individuals (i.e. the sender and recipient). In symmetric-key cryptography, the sender and receiver of the message must share the same key. In modern cryptography, the key is a long string of bits. The distribution or agreement of keys are crucial to data confidentiality.

Even though the algorithms currently in use (e.g. the DiffieHellman key agreement protocol [2]) are able to establish a shared secret key over an insecure communications channel, they are vulnerable to some types of attacks. Nowadays, the solution which ensures the highest level of security is quantum key distribution.

The key distribution algorithms currently in use are able to establish a shared secret key over an insecure communications channel. The security of these algorithms is based on the fact that successful eavesdropping requires excessive computational effort. Quantum cryptography brings an entirely new way of solving the key distribution problem. It provides secure key distribution via the laws of quantum mechanics [3].

First of all, the rules of quantum mechanics ensure that any measurement modifies the state of the transmitted qubit (quantum bit). This modification can be discovered by the sender (Alice) and the receiver (Bob) of the quantum bits. In that way, passive eavesdropping is not possible – when an eavesdropper (Eve) wants to listen to photons, she will change their quantum states (in addition, Eve is not able to clone the unknown photon state).

Quantum key distribution (QKD) is used to distribute an encryption key for symmetric ciphers but not to transmit any message data between users. Today, a lot of QKD protocols have been created, but few are used in practice [4]. The first invented protocol was BB84 [5]. This protocol, based on single particles (polarized photons), is the most popular solution in practice. Many other protocols, such as BBM92 [6] or SARG04 [7] are modified versions of the BB84 protocol.

A. BB84 protocol

In common with many papers related to cryptography, we introduce three characters: Alice (usually the sender) and Bob (usually the receiver) – individuals who want to communicate confidentially – as well as Eve, an eavesdropper. In a typical scenario, Alice and Bob want to establish a secret key and Eve wants to gain information about this key.

When Alice wants to establish a new encryption key with Bob, they both have to define two alphabets: rectilinear and diagonal. Let us assume that, in the rectilinear alphabet, photons with horizontal polarization 0° mean bit 0 and photons with vertical polarization 90° mean bit 1. Similarly, in the diagonal alphabet, photons with polarization -45° mean bit 0 and photons with polarization 45° mean bit 1. In Fig. 1 the double-headed arrows represent the polarization states of individual photons.

If we observe one photon with diagonal polarization 45° using the rectilinear basis, the photon 'chooses' one of the

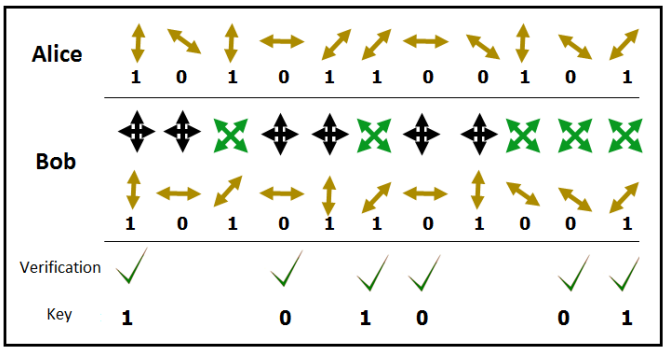


Fig. 1. An example of the BB84 protocol

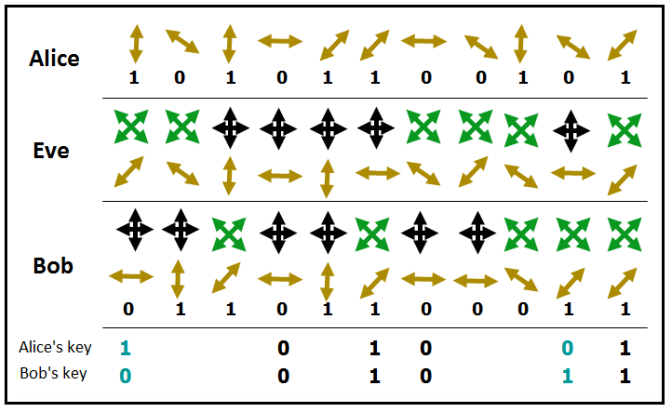


Fig. 2. Eavesdropping in the BB84 protocol

polarizations: horizontal or vertical with probability $\frac{1}{2}$. This means that we are only able to perfectly measure photons with polarization $0°$ and $90°$ by means of a detector oriented in the vertical/horizontal directions (called rectilinear basis). We lose information about diagonally polarized photons ($-45°$ and $45°$). Similarly, using the a diagonal basis we are only able to perfectly measure only photons with polarization $-45°$ and $45°$. In this situation, we lose information about horizontally and vertically polarized photons ($0°$ and $90°$) In Fig. 1, two crossed double headed arrows: $0°$ and $90°$ mean rectilinear basis (black). Similarly, two crossed double headed arrows: $-45°$ and $45°$ mean diagonal basis (green).

At the beginning of the protocol operation, Alice sends Bob a string of bits which is encoded by means of photons polarization (qubits). Alice sends the bits using a randomly chosen alphabet, via a quantum channel. Bob receives this string using rectilinear basis (enabling perfect detection of polarizations: $0°$ and $90°$) or diagonal basis (enabling perfect detection of polarizations: $-45°$ and $45°$). Bob chooses the basis randomly, but then informs Alice which he used. He sends this information on a public channel. It is worth emphasizing that Bob only discloses only information about the basis used. The result of the measurement is secret. Now, Alice informs Bob when he has chosen the proper basis to measure the photon. The new key consists of those bits for which Bob has chosen the basis correctly, because they then both have the same bits.

In the example presented in Fig. 1, the first photon is detected perfectly and will be the first bit of the new key. Alice and Bob have to reject the second and third bits because Bob chose the wrong basis and the polarization measurement is uncertain. The next bit (fourth) is detected perfectly and will be part of the key. An algorithm such as this ensures that the distributed key consists of approximately half of the bits sent by Alice. Alice and Bob must disregard the other 50%.

Now, let us assume that Eve eavesdrops on the communication between Alice and Bob via the quantum channel. In Fig. 2, an example of key distribution with eavesdropping is presented.

To obtain information, Eve has to measure the polarization of photons using rectilinear or diagonal basis. She chooses the basis randomly (like Bob) but if the chosen basis is incorrect, the polarization will be changed. Such an effect is presented in Fig. 2: originally the first bit has a vertical polarization (coded bit 1), but Eve eavesdrops using a diagonal basis and after that the photon has the polarization $45°$. After Bob's measurement, this photon has a horizontal polarization and will be decoded as 0. Even though Alice sent the vertically polarized photon and Bob selected the proper rectilinear basis, they obtained different bits. Therefore, if Alice and Bob compare the part of the key obtained in the public channel, they uncover eavesdropping.

As a result, passive eavesdropping is not possible – when Eve wants to eavesdrop photons, she will change the quantum states of the photons. Besides, Eve is not able to clone an unknown state of the photon. Therefore, the BB84 protocol ensures a high level of security.

B. Key distillation

During the quantum key distribution process, Alice and Bob use two communication channels: quantum and public. In the quantum channel, information is coded using quantum states. In the public channel, Alice and Bob exchange data to check whether Eve was eavesdropping. The public channel is generally necessary for a significantly greater number of cases.

Eve is not the only one responsible for errors in the quantum channel. Errors during quantum communication may occur for reasons such as disturbance in the quantum channel, optical misalignment, or noise in detectors. The number of errors in contemporary QKD systems comprises a few percent of all bits. This contrasts strongly with the Bit Error Rate (BER) in standard communication networks where the typical value is at the level of 10^{-9}. In order to avoid confusion, we refer to the number of errors in QC as the Quantum Bit Error Rate (QBER). The QBER is defined as the ratio of the number of wrong bits to the total number of bits [8]. In general, the QBER can be calculated from the following formula:

$$QBER = \frac{\text{Number of errors}}{\text{Total number of bits}} * 100\% \qquad (1)$$

Due to errors, Alice and Bob have to estimate the error rate and decide whether there is an eavesdropper. In practice, they

compare a small portion of a raw key distributed through the public channel and compute the QBER. If the QBER exceeds a given threshold, it means that Eve has eavesdropped (or the quantum channel is too noisy to perform a proper key distribution). However, if the error rate is low enough, Alice and Bob continue to distil the key further. Naturally they must delete the compared part of the raw key.

After the bit error estimation, Alice and Bob use key distillation protocols. These protocols usually involve two steps: key reconciliation and privacy amplification.

As mentioned previously, quantum communication is not perfect and some errors do occur. If the number of errors does not exceed a given QBER threshold, the reconciliation process must find and correct or delete these errors. The simplest solution is the parity test. The key is divided into several blocks, and Alice and Bob compare the parity of each block. If the parity does not agree, they know that an error occurred and continue searching for the error by dividing the block into two parts. The algorithm is repeated until the error is corrected or deleted. Unfortunately, following the parity test, Alice and Bob must reject one bit to reduce Eve's knowledge about each block. This way the key is shortened again, but Alice and Bob will be sure that they have the same string of bits (without errors).

At the end of the key distillation process, the privacy amplification should be carried out. Because Eve may have gained significant knowledge of the key (eavesdropping in the quantum channel and in the public channel during the bit error estimation and key reconciliation), Alice and Bob are required to strengthen their privacy. They can delete some of the bits and construct the final key in a specific way.

If Alice and Bob perform all the steps considered here, the final key which can be used for symmetric encryption is reduced. This reduction of the key length is characteristic for all quantum key distribution protocols. Let us assume that the length of raw key obtained from quantum channel is Q, the length of the key after the bit error estimation is B, the length of the key after key reconciliation is R, and the length of the final key (after the privacy amplification process) is A. Then we can present the reduction of the key lengths at different steps as follows:

$$Q > B > R > A \tag{2}$$

Because each stage reduces the key length, the performance of the QKD is also reduced. Sometimes, when we want to ensure a high level of security, this reduction is significant. This is the reason why end-users need methods which can measure and manage security. These solutions are crucial to quantum cryptography implemented in real communication networks.

III. The measure of security

Let us assume that we have a string of bits B which is an encryption key distributed using a QKD protocol from Alice to Bob:

$$B = [b_1, b_2, \ldots, b_n] \tag{3}$$

The key is distributed using quantum states of photons. When Bob receives qubits from Alice and obtains the encryption key, he is not sure whether B is really secure. Therefore, Alice and Bob have to uncover some bits to know that eavesdropping occurred. Each bit can be confidential – it means that nobody was eavesdropping – or not. However, the crucial question is how many bits they need to uncover to know that the encryption key is really secure.

When Alice and Bob uncover one bit, the information about security of the key B increases. Because the key length is n, the probability that we uncover bit b_i is $\frac{1}{n}$. It also means that we uncover and compare $\frac{1}{n} * 100\%$ of the key.

Now let us assume that J is a function which indicates that the key was not eavesdropped on during the quantum key distribution process. Such function J could be the measure of security of the binary string B because it directly influences data confidentiality.

If we assume that k is the number of uncovered bits, the function $J(k)$ is monotonously growing; this means that if k is increasing, then $J(k)$ is also increasing. According to a real scenario, the more bits we compare, the more we know about security of the distributed encryption key.

Intuitively, function $J(k)$ should not be linear. Let us consider the uncovered bits first: just a few first bits are sufficient to obtain general information about the security of the distributed key. Therefore, these first bits provide more information about the security of the key than the same number of bits that have been uncovered later (especially when bits in a key are checked at random).

The function $J(k)$ defined this way has the following properties:

- if we uncover 0 bits, we know nothing about the key security (the minimum knowledge about security),
- if we uncover all bits (n bits), we are sure whether the key is secure or not (the maximum knowledge about security).

The function $J(k)$ which meets these requirements can be defined as the following logarithmic function:

$$J(k) = \log\left(\frac{k}{n}\right), \tag{4}$$

where log represents the natural logarithm – the logarithm with the base e. The constant e is called Euler's number and is equal to approximately: $e \approx 2.71828$. The function $J(k)$ has the analogous form with the measure of information introduced by Hartley in 1928 [9]. In Fig. 3, an example of function $J(k)$ was presented where the key length is 1000 bits.

It should be noted that the measure of security is similar to the measure of information, although they are not the same. First of all, in QC we uncover the bits one by one, therefore the elements are always in a strict order:

$$\psi = \{\textbf{one } uncovered\ bit, \ldots, \textbf{n } uncovered\ bits\}. \tag{5}$$

Additionally, probabilities assigned to the elements are always in a strict order:

$$\phi = \left\{\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}, 1\right\}. \tag{6}$$

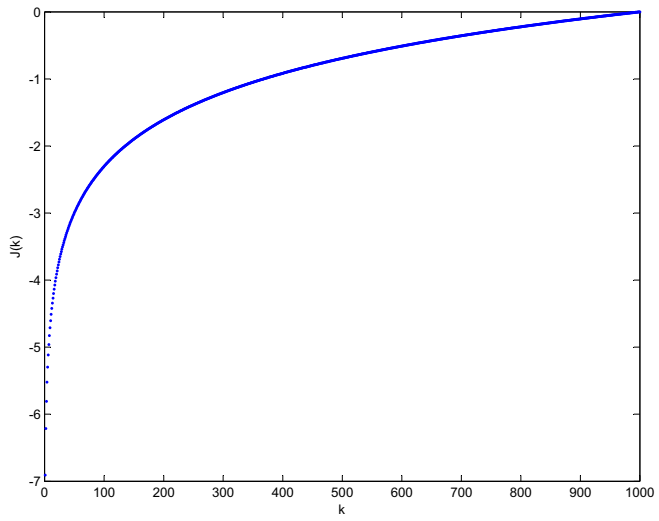


Fig. 3. An example of function J(k) for key length: 1000 bits

The function $J(k)$ defined by Equation (4) has the following domain X and codomain Y:

$$X \in \{1, 2, \ldots, n\} \quad and \quad Y \in (-\infty, 0]. \tag{7}$$

Now let us modify the function $J(k)$ because of the range of the codomain. The codomain presented in Equation (7) is not intuitive for end-users, and could be inconvenient for some applications. Additionally, the measure should not be a negative number (the non-negativity property of the measure in the measure theory). Therefore, we can define the function $\widehat{J}(k)$ which has values between 0 and 1. This codomain can also be easily transformed to the range 0% to 100%. The function $\widehat{J}(k)$ can have the following format:

$$\widehat{J}(k) = \frac{\log(k+1)}{\log(n+1)} \tag{8}$$

Additionally, Equation (8) can be simplified to:

$$\widehat{J}(k) = \log_{n+1}(k+1) \tag{9}$$

This means that the security of QC depends on the number of uncovered and compared bits (k). The numerator in Equation (8) presents the growing function $\widehat{J}(k)$, and the denominator limits the value of $\widehat{J}(k)$ to 1. It should be noted that:

- the minimum value of the function $\widehat{J}(k)$ is 0 (we uncovered 0 bits and we have the minimum knowledge about security: $k = 0$), and
- the maximum value of the function $\widehat{J}(k)$ is 1 (we uncovered the all bits and we have the maximum knowledge about security: $k = n$).

When we observe the function $J(k)$ in Fig. 3, we can say that the measure of security is increasing strongly when we compare the first 20% bits. When we want to compare the last 30% bits (from 70% to 100%), we only get a small improvement of the $J(k)$ value.

IV. Entropy of Security

Now, let us develop the idea of quantity of security. By analogy to the Shannon's entropy, we can define:

$$S(\psi) = -\sum_{k=1}^{n} p_k * J(k) = -\sum_{k=1}^{n} \frac{k}{n} * \log\left(\frac{k}{n}\right) \tag{10}$$

as the *entropy of security*. It is the average measure of security included in a single element of ψ. $S(\psi)$ defines the average security of the key when we uncover and compare k bits. The minus sign in Equation (10) ensures the positive values of $S(\psi)$.

Also, we can define the function of the *entropy of security*:

$$S(k) = -p_k * J(k) = -\frac{k}{n} * \log\left(\frac{k}{n}\right) \tag{11}$$

Fig. 4 shows an example graph (with a key length of 1000 bits) of $S(k)$.

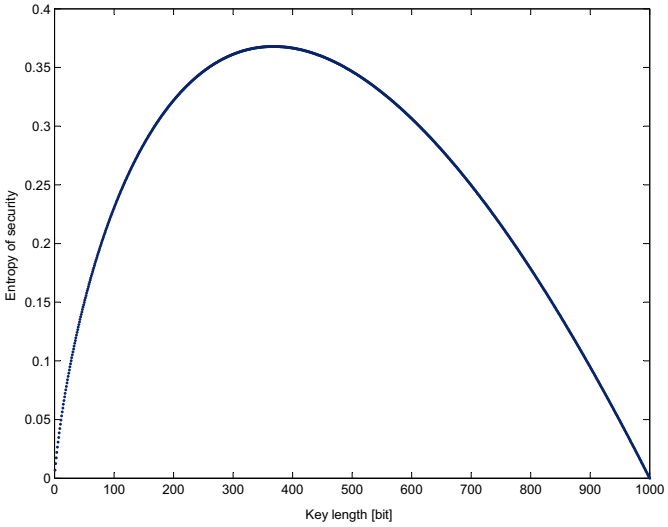


Fig. 4. An example of function $S(k)$ (key length: 1000 bits)

The function $S(k)$ defined by Equation (11) has one global maximum. In order to find it, we have to calculate the derivative of the function $S(k)$:

$$S'(k) = \frac{d}{d\,k} S(k) = -\frac{1}{n} log\left(\frac{k}{n}\right) - \frac{1}{n}, \tag{12}$$

and equate the derivative to 0:

$$\frac{d}{d\,k} S(k) = 0 \quad \Rightarrow \quad k = e^{log(n)-1}. \tag{13}$$

Equation (13) can be simply transformed to the following expression:

$$k = \frac{n}{e}. \tag{14}$$

It should be noted that the calculated extremum of $S(k)$ does not depend on the base of the logarithm in the function $S(k)$. Therefore, we are able to define a very general principle that the maximum of the function of *entropy of security* is

always equal to $\frac{n}{e}$. If we then divide the maximum of this function by n (the number of bits), we obtain the number:

$$\frac{1}{e} \approx 0.3679 \tag{15}$$

This means that the maximum of function $S(k)$ corresponds to the situation when we uncover and compare approx. 37% bits of the key.

Now let us consider the *entropy of security* defined in Equation (10). The entropy $S(\psi)$ depends on the number of bits n in the given key. However, we can observe the following relationship:

$$\lim_{n\to\infty} \frac{S(\psi)}{n} = \lim_{n\to\infty} \frac{\sum_{k=1}^{n} S(k)}{n} = 0.25 \tag{16}$$

Therefore, 0.25 is the maximum value of *entropy of security* divided by the number of bits in the key. The values of the function:

$$\widehat{S}(k) = \frac{\sum_{k=1}^{n} S(k)}{n} \tag{17}$$

are included in the interval $(0\,,\,0.25)$. It does not depend on the number of bits in the key. Therefore, we have a general relationship which we can use to measure the security of QC.

The function presented in Equation (17) has a practical application in high-level communications protocols and services. This function makes it possible to control the security of the encryption key by end-users, and improve the practicality and efficiency of the security measurement. If we want to manage security in high-level services, we can create specific security levels of the quantum cryptography. Using the *entropy of security* enables us to influence network services to meet specific end-user security requirements [10].

Let us analyze the features of function $S(k)$. First we calculate the sum of S(k) values (*entropy of security*) from the first element $k = 1$ to the maximum of the function:

$$\lim_{n\to\infty} \widehat{S}_A(k) = \lim_{n\to\infty} \frac{S(k)}{n} \approx 0.1015 \tag{18}$$

We can mark this point (called point A) in the graph of entropy of security. It should be noted that in the considered interval, the function is growing (the values of *entropy of security* increase).

We also need to define the minimum value of entropy of security. This value defines a minimum number of compared bits during the QBER estimation process. A lower number may not uncover eavesdropping. This additional point is called as point B.

Now, let us analyze the function $J(k)$. The function $J(k)$ increases powerfully from 0 to the point B and reaches the minimum security from point B. Therefore, if we define the point B as:

$$\lim_{n\to\infty} \widehat{S}_B(k) = 0.01 \tag{19}$$

we can state that:

$$\widehat{S}(k) \leq 0.01 \tag{20}$$

defines the unsecured QC system where we are not able to uncover an eavesdropper.

These values give us an opportunity to specify the security levels in the QC system. We propose two security levels which are dedicated to specific high-level services. Using these levels, we can personalize the security for specific end-users and services.

- **Basic security**
  Already from 8% to 37% compared bits are sufficient to collect information about security of a distributed key. Therefore, it should be sufficient for personal use of quantum cryptography as well as some ordinary commercial services. This level of security ensures that the value of the $\widehat{S}(k)$ function is not lower than 0.01 but not greater than 0.10:
  $$0.01 \leq \widehat{S}(k) \leq 0.10 \tag{21}$$
- **Advanced security**
  We can imagine certain services which require the highest security level, e.g. essential bank communications, police services or even the military use of QC. For these services, the value of the function $\widehat{S}(k)$ should be greater than 0.10:
  $$\widehat{S}(k) > 0.10 \tag{22}$$

Fig. 5 presents the function $J(k)$ (the measure of security) and the function $S(k)$ (the entropy of security), respectively. The security levels as well as points A and B are marked on the graphs.

V. Verification

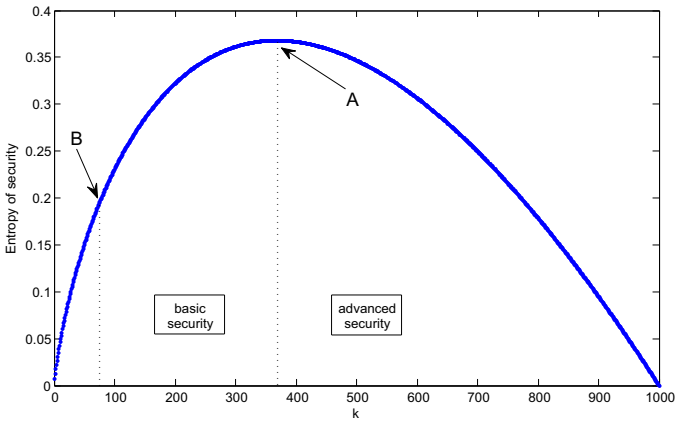
The functionality of the proposed approach was implemented in a QKD simulator. The simulator is written in C++ and available under the general public license. More details on the simulator were shown in [11].

The simulator calculates the difference between real values of QBER (called *true_QBER*) and QBER calculated using the presented method (called *measured_QBER*). The *true_QBER* is the ratio of the number of eavesdropped bits to the total number of bits in the key. If we knows the number of wrong bits and the total number of bits in a key, the QBER can be easy calculated using Equation (1). The following formula is computed following each simulation:

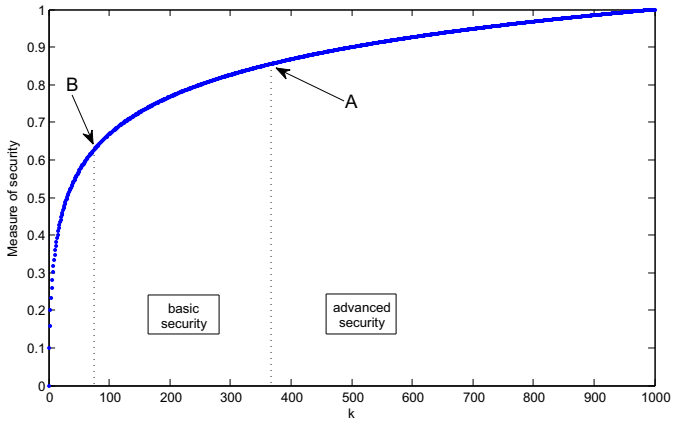
$$|true\_QBER - measured\_QBER| \tag{23}$$

We simulated keys with 1000 bits which are distributed by the BB84 protocol. During the simulations, Eve is eavesdropping on different numbers of bits, ranging between one and 1000 bits. Therefore, 1000 simulations are performed in a single step. Numerous simulations were performed to verify the differences between *true_QBER* and *measured_QBER* for different values of function $\widehat{S}(k)$. Finally, approximately 1.5 million single transmissions of a key between Alice and Bob were simulated. The results of the verification are shown in Fig. 6.

It is clear that the functions in the graphs are decreasing, with the most significant changes observed in the interval $(0\,,\,0.10)$ (the basic security). Smaller changes are observed in the interval $(0.10\,,\,0.25)$ (the advanced security).



(a)



(b)

Fig. 5. Security levels on the graph of (a) the entropy of security, (b) the measure of security

Fig. 6 presents the results of simulations without the noise in the quantum channel. Nevertheless, additional simulations confirmed that the curves for noise intensity 2% and 5% are similar. More simulation results were presented in [1]. It should be noted that all curves are linear in the advanced security level; however, the curves in the basic security level are exponential. This means that in the basic security level, the security of a key increases faster than in the advanced security level. The results confirmed the theoretical considerations.

VI. Conclusion

In this paper, the new concept of measure of security in QC was proposed. It was shown that based on the quantitative approach to security, measurement and assessment of security is possible. The measure of security and proposed entropy of security were presented in detail. Additionally, end-users are able to personalize the security in the QC system depending on requirements. Therefore, the method allows us to manage the quantity of security depending on specific end-user requirements and needs. Finally, the proposed solution was verified by the performed simulations.

Interest in quantum cryptography is growing rapidly. We still observe new implementations of QKD and new network services supported by this technique. The next step will be the integration of QC services with real networks. Then, end-users will need the methods which allow us to control the security in systems using QC. The candidate for such a method was presented in this paper.

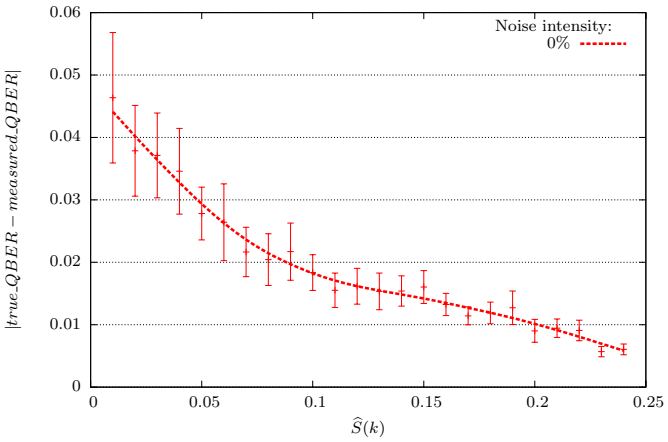


Fig. 6. Simulation of QBER (noise = 0%)

Acknowledgment

This work has been co-financed by the INDECT project funded by European Community's Seventh Framework Programme under grant agreement no. 218086.

References

[1] M. Niemiec, "Design, Construction and Verification of a High-Level Security Protocol Allowing to Apply the Quantum Cryptography in Communication Networks," 2011, Ph.D. Thesis, AGH University of Science and Technology, (supervisor: prof. Andrzej R. Pach).

[2] RFC2631, "RFC2631: Diffie-Hellman Key Agreement Method," June 1999.

[3] D. Bouwmeester, A. Ekert, and A. Zeilinger, *The Physics of Quantum Information. Quantum Cryptography, Quantum Teleportation, Quantum Computation*. Springer, 2000.

[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Reviews of Modern Physics*, vol. 81, pp. 1301–1350, 2009.

[5] C. H. Bennett and G. Brassard, "Public key distribution and coin tossing," *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, pp. 175–179, 1984.

[6] C. H. Bennett, G. Brassard, and D. N. Mermin, "Quantum cryptography without Bell's theorem," *Physical Review Letters*, vol. 68, 1992.

[7] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Physical Review Letters*, vol. 92, 2004.

[8] M. Sharifi and H. Azizi, "A Simulative Comparison of BB84 Protocol with its Improved Version," *Journal of Computer Science and Technology*, vol. 7, 2007.

[9] R. V. Hartley, "Transmission of information," *Bell System Technical Journal*, vol. 7, pp. 535–563, 1928.

[10] M. Niemiec, "Quantum cryptography - the analysis of security requirements," in *Transparent Optical Networks, 2009. ICTON '09. 11th International Conference on*, 2009.

[11] M. Niemiec, L. Romanski, and M. Swiety, *Quantum cryptography protocol simulator*, ser. Multimedia Communications, Services and Security, Communications in Computer and Information Science. Springer, 2011, vol. 149, pp. 286–292.