Universität Rostock Traditio et Innovatio

Baltic Young PhD Conference

10. Baltische Sommerschule
„Technische Informatik /
Informationstechnik“

BaSoTI 10 in Riga

Konferenz
28. – 29.07.2014

Baltic Young PhD Conference

Riga, 28.-29.07.2014

Universität Rostock 2014

Herausgeber: Prof. Dr. Clemens Cap
Wissenschaftsverbund „Informations- und Kommunikationstechnologien“ (IuK)

Erstellung der Druckvorlage: André Sandmann

Entwurf des Umschlagbildes: Christine Bräuning

Bezugsmöglichkeiten: Universität Rostock
Institut für Informatik
Frau Jacqueline Tiedemann
Albert-Einstein-Str. 22, Raum 356
18059 Rostock

Universität Rostock
Wissenschaftsverbund IuK
Frau Dr. Christine Bräuning
Albert-Einstein-Str. 22, Raum 364
18059 Rostock

Druck: IT- und Medienzentrum der Universität Rostock

Table of Contents

Preface

Due to the generous support of the German Academic Exchange Service (DAAD - Deutscher Akademischer Austausch Dienst), BaSoTI summer school is going in to its tenth year, with the associated conference going into its eighth year.

It was in 2005, that the University of Bremen, the University of Lübeck, the International School of New Media at the University of Luebeck (ISNM), and the University of Rostock joined forces for the first Baltic Summer School in Technical Informatics (BaSoTI). Supported by a sponsorship of the German Academic Exchange Service a series of lectures was offered between August 1 and August 14, 2005 at Gediminas Technical University at Vilnius, Lithuania. The goal of the Summer School was to intensify the educational and scientific collaboration of northern German and Baltic Universities at the upper Bachelor and lower Master level.

In continuation of the successful programme, BaSoTI 2 was again held at Vilnius in 2006 and 2009, BaSoTI 3 took place in Riga, Latvia at the Information Systems Management Institute in 2007, BaSoTI 4, BaSoTI 5 and BaSoTI 8 were held at the University of Tartu, BaSoTI 6 took place in Kaunas, Lithuania and BaSoTI 7 and BaSoTI 10 at the Technical University of Riga, Latvia.

Since BaSoTI 3, the Summer School lectures have been complemented by a one day scientific event. The goal is to give young, aspiring PhD candidates the possibility to learn to give and to survive an academic talk and the ensuing discussion, to get to know the flair and habits of academic publishing and to receive broad feedback from the reviewers and participants. Moreover, the Summer School students would have a chance to participate in what most likely would be their first academic research event.

In 2014, the year of the tenth anniversary of the BaSoTI the conference was addressed to young PhD candidates from the Baltic States and the German partner universities especially. Moreover, international, reviewed contributions by researchers were presented and BaSoTI students contributed with short talks on their work.

Clemens H. Cap

Rostock, November 2014.

Programme Committee

Ahrens, Andreas (University of Technology, Business and Design Wismar, Germany)

Cap, Clemens (University of Rostock, Germany)

Kemmerich, Thomas (Høgskolen i Gjøvik, Norway)

Mundt, Thomas (University of Rostock, Germany)

Pfisterer, Dennis (Baden-Wuerttemberg Cooperative State University Stuttgart, Germany)

Sobe, Peter (University of Applied Sciences Dresden, Germany)

Low Power Algorithm for Shoe Mounted Inertial Navigation System

Ramunas Adamonis
Faculty of Electronics
Vilnius Gediminas Technical University
Vilnius, Lithuania
email: ramunas.adamonis@stud.vgtu.lt

Abstract: Inertial navigation systems are adopted in various scenarios where systems cannot rely on external reference source. In this work to create an algorithm for human movement tracking acceleration and magnetic field signals are used. The present work addresses problems of human walking pattern recognition, heading estimation, specially with possible tilt compensation and step length estimation from accelerometer data. All problem solutions are combined into one algorithm. Finally algorithm was tested to check the performance of low power algorithm.

1 Introduction

Indoor localization had recently become a field of great interest. Inertial sensors, RFID, WLAN and other similar technologies allows to improve GNSS-based navigation systems, specially indoors, where system cannot rely on stable GNSS signal. Furthermore small dimensions and high computational power enables to integrate navigation system hardware into already existing equipment without major modification of equipment itself. This vastly increase possible applications for indoor navigation system. As an example could be widely applied idea to use indoors navigation system for firefighters. More about this application can be read in [FG10] article. From here the biggest challenge of localization system can be derived. When indoors navigation system does not have a reference points, such as RFID tags or WLAN transmitters, only recursive algorithms can be used and it causes drift of a system over time. Despite that a lot of scientists are trying to apply new solutions and improve reliability of the indoor navigation.

Although importance of reliability cannot be denied, in this work another perspective will be considered and that is power consumption. System has to be not only reliable, but also power efficient to provide autonomous behavior. And one of the possibilities to achieve this is to power it by autonomous power supply. Such example could be human motion energy harvester (for further information please see [KHFM40]). But the problem is that such energy harvester is capable to produce power which is in few milliwatts order, while most of current localization systems consumes far greater amount (statement based on power consumption level measured for system described in [RGAJ+12]). In this work low-power algorithm will be developed to achieve as low power consumption as possible.

Due to conserving power, some solution will be directed not to best result, but to lowest power consumption.

For sensor data recording Xsens MTw development kit was used. It is a commercial device popular between researches for its high accuracy and plug and play capability. Moreover sensors are calibrated by manufacture with large precisions, which allows use this kit without major preparations.

For data processing and algorithm creation Matlab computing environment was used. Matlab is a high-level language and interactive environment for numerical computation, visualization, and programming. It is developed by company Mathworks.

2 Step detection

In most of simple algorithms for pedestrian navigation step detection is corner stone of the algorithm. In this work step detection will also be the first goal. After detecting the step other properties can be calculated. In this case some computational power can be saved while human is not moving.

For step detection 3D accelerometer is used. In this case acceleration is measured in three different axis: x, y and z (a_x, a_y, a_z). Since sensor unit position is not predefined it is not wise to use measurement from only one axis so in order to get robust step detection, norm of acceleration is calculated Eq. 1.

$$a_n = \sqrt{a_x^2 + a_y^2 + a_z^2} \tag{1}$$

At this point norm of acceleration consists of measured acceleration and acceleration of gravity Eq. 2.

$$a_n = a_N + a_g \tag{2}$$

For further processing acceleration of gravity should be removed. There is somel ways to do it:

- By calculating the mean value of acceleration and then subtracting it from current measurement:
$$a_N = a_n - (\sum_{j=1}^{M} a_n)/M) \tag{3}$$
- Applying simple low pass filter:
$$a_N = a_n - a_{n-1} \tag{4}$$
- Simply subtracting the constant gravity constant from the measured data:
$$a_N = a_n - a_g \tag{5}$$

In this algorithm constant subtraction in used in order to avoid additional calculations Eq. 3.

Acceleration signal obtained at this moment is shown in figure. 1.

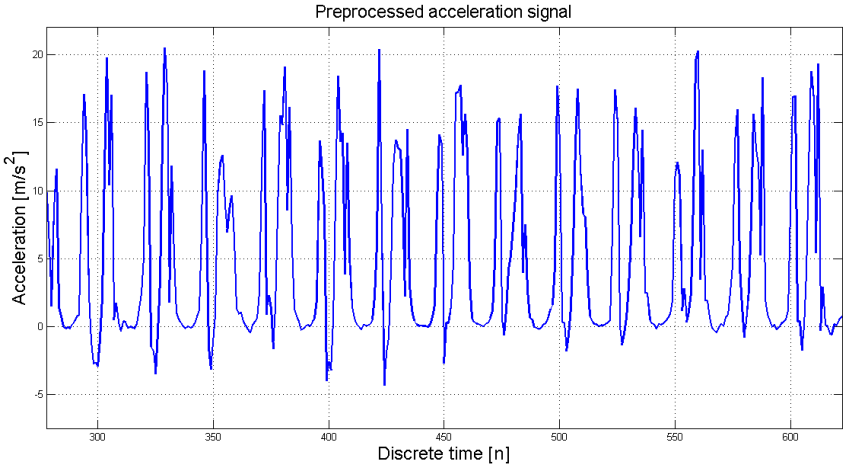


Figure 1: Norm of acceleration without the constant of gravity.

Once proper signal is obtained the step detection algorithm can be applied. There are many algorithms used to detect steps [YSS+07], [CP06].

In this work peak detection algorithm was chosen to be implemented into this system since it is one of the simplest algorithm and requires small amount of computational power. Even simply detecting peaks works using a threshold works, but some steps are being missed because of signal noise, or unusual walking pattern. So to detect peak, acceleration signal must be preprocessed.There are many techniques for doing so in [MGW+08], but in this case different approach was chosen. First of all absolute value of signal is calculated, in this case negative acceleration peaks becomes positive.

$$a_{aN} = |a_N| \tag{6}$$

In next step. the threshold is applied. Threshold main purpose is to ignore all acceleration values which are lower than specific value, which is usually found by checking experimental data. Main reason to use threshold is that even when the foot is standing still, there are some vibrations captured by accelerometer, moreover gravity constant might slightly vary depending on which place on earth you are. Threshold helps to avoid these small chances in acceleration, and focus only on real data. The easiest way to find a threshold values is to look at experimental data. In figure 2 there is the acceleration signal with applied threshold, lower boundary is 1, and upper boundary is 2, upper boundary is used just to clearly show the effect of threshold. As it can be seen, there is a clear pattern between steps. It is possible to observe that step is usually represented of two spikes, followed by

a space, in which foot is still. Now a mechanism is needed to clearly recognize the step peak. In this work a sliding window smoothing mechanism is applied. Principle of sliding window is shown in figure 3. If the low threshold value is found between high values it is changed to artificial high value. In this way step is being represented by one spike which is equal to upper threshold. Because of the sliding window, the delay will occur, and will be proportional to length of the window and sampling frequency. At this point sample length of the step can be easily calculated by simply calculating length of the peak. By applying minimal sample length for the step detection it can be assured that step would not be mixed with random noise. Minimal sample length can by found from experimental data.

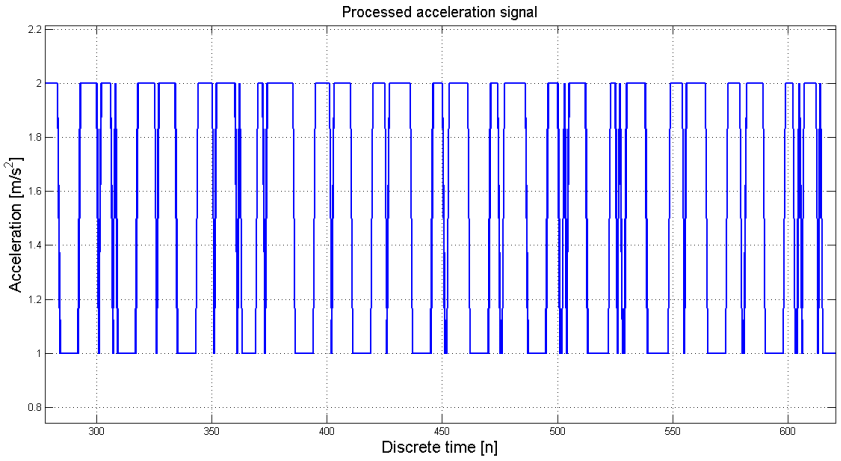


Figure 2: Acceleration signal with applied threshold.

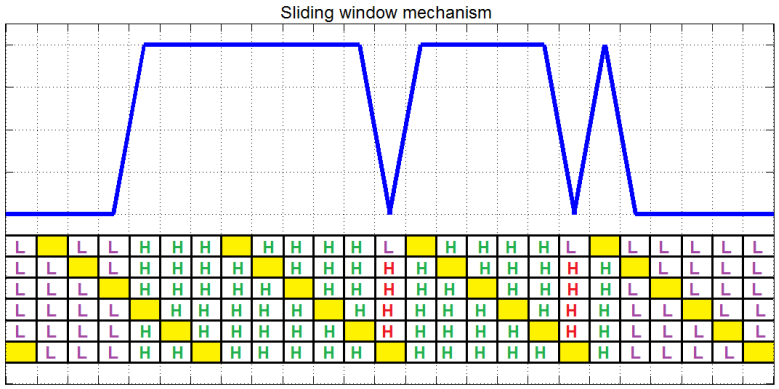


Figure 3: Sliding window mechanism.

By now algorithm works simply checking if the value of acceleration is high, if so it starts to calculate the samples, and when it reaches point when accelerations is low again, it indicates that the step was found. Although the algorithm has a simple structure, it should be robust enough to find steps in normal walking pattern. On the other hand if walking speed would be high enough, the steps could merge to each other and algorithm could fail. Also if walking speed would be too slow, the step could be over detected, and instead of one step multiple steps could be found.

3 Heading estimation

Usually heading is estimated from data provided by gyroscope, or by gyroscope and magnetometer. But gyroscope consumes by far more power compared to magnetometer, mainly because its principle of operation (Coriolis effect) and only magnetometer is left to be used for heading estimation. Of course in this case results of complete system will be far worse, that in those approaches which uses gyroscope, but it is the price one has to pay in order to create a navigation system, with low power consumption. Since gyroscope will not be used, not many choices are left for heading estimation. Easiest way is to simply calculate heading angle from magnetometer data by using equation 7:

$$\psi = arctan\left(\frac{m_y}{m_x}\right) \tag{7}$$

where ψ is angle of z axes, m_y is magnetic measurement on y axes and m_x is magnetic measurement on x axes

Although this equation is correct in order to have correct readings the angle of x axis (ϕ) and y axis (θ) should be zero. And in this case it might happen that sensor placed on a shoe would be tilted. To solve this problem tilt compensation should be applied. Or in the other words sensor should be rotated from local frame to global frame. To do so angles of sensor tilt is required. Easiest way to get these angles is to use acceleration data, since it is already used for step detection. It can be done by using following equations:

$$\phi = arctan\left(\frac{a_y}{a_z}\right) \tag{8}$$

$$\theta = arctan\left(\frac{a_x}{a_z}\right) \tag{9}$$

Once angles are obtained, rotation matrices can be calculated. Author in [Kon08] present method for tilt compensation using rotation matrices, those matrices will be used in this work. Rotation about x axis can be expressed as:

$$R_\phi^x = \begin{bmatrix} 1 & 0 & 0 \\ 0 & cos\phi & sin\phi \\ 0 & -sin\phi & cos\phi \end{bmatrix} \tag{10}$$

where R_ϕ^x is rotation through an angle ϕ about x axis.

And rotation about y axis can be expressed as:

$$R_\theta^y = \begin{bmatrix} cos\theta & 0 & -sin\theta \\ 0 & 1 & 0 \\ sin\theta & 0 & cos\theta \end{bmatrix} \tag{11}$$

where R_θ^y is rotation through an angle θ about y axis.

Rotation to global frame can be achieved by applying these matrices one by one or by calculating and applying product of the matrices:

$$R = R_\phi^x R_\theta^y = \begin{bmatrix} cos\theta & 0 & -sin\theta \\ sin\phi sin\theta & cos\phi & sin\phi cos\theta \\ cos\phi sin\theta & -sin\phi & cos\phi cos\theta \end{bmatrix} \tag{12}$$

In order to apply rotation to magnetic measurement it is enough to simply calculate product of rotation matrix and measurement data:

$$\begin{bmatrix} m_{comp\_x} \\ m_{comp\_y} \\ m_{comp\_z} \end{bmatrix} = R \begin{bmatrix} m_x \\ m_y \\ m_z \end{bmatrix} \tag{13}$$

where m_{comp_x}, m_{comp_y}, m_{comp_z} is tilt-compensated magnetic measurements in x, y, and z axes.

Once new, tilt-compensated, measurement are obtained, tilt-compensated heading can be calculated:

$$\psi_{comp} = arctan\left(\frac{m_{comp\_y}}{m_{comp\_x}}\right) \tag{14}$$

where ψ_{comp} is tilt-compensated heading

4 Step length estimation

Low power pedestrian navigation system could already operate, just by applying constant step length. But in such case, there is a risk, that system would drift to much if there walking pattern would not be constant. In order to solve this problem, a step length estimation can be adopted to the system. Authors in [JBS+10, AGLA06] compare well known step length estimation algorithms. Although they show quite good results, both of reviews are not about foot wear devices, and while they still approximate step length, some of their performance in this case (foot wear device) is not as good as expected while others require too many calculations. So in this case different approach was chosen.

First raw data was recorded. Then this data was processed with "ZUPT" [RGK+13] algorithm. Since "ZUPT" gives quite good step length estimation, this step length was chosen for the reference. After that raw data was assigned to corresponding step and different processing for this data was applied. Finally polynomial curve fitting was applied to check which data processing method gives lowest sum of square errors. First order curve fitting was chosen since it requires least number of computations. The following methods were chosen for best performance:

Variance of acceleration - Variance shows how much a current measurement differs from the average. It can be calculated using following equation:

$$\sigma^2 = \frac{\sum_{n=1}^{N} [a_n - \bar{a}_n]^2}{N-1} \tag{15}$$

where N is number of acceleration samples during a step, a_n is current acceleration measurement and $\bar{a_n}$:

$$\bar{a_n} = \bar{a}_{n-1} + \frac{1}{n}(a_n - \bar{a}_{n-1}) \tag{16}$$

here average must be calculated recursively because system should run on a real time.

After calculating variance, "Matlab" built-in curve fitting tool can be used to approximate function between step length and variance of acceleration. Data points which are under 0.8 meters are excluded in this fitting, because it is not likely that step length could be smaller in a normal walking pattern. First order polynomial $(ax + b)$ is used to fit data points

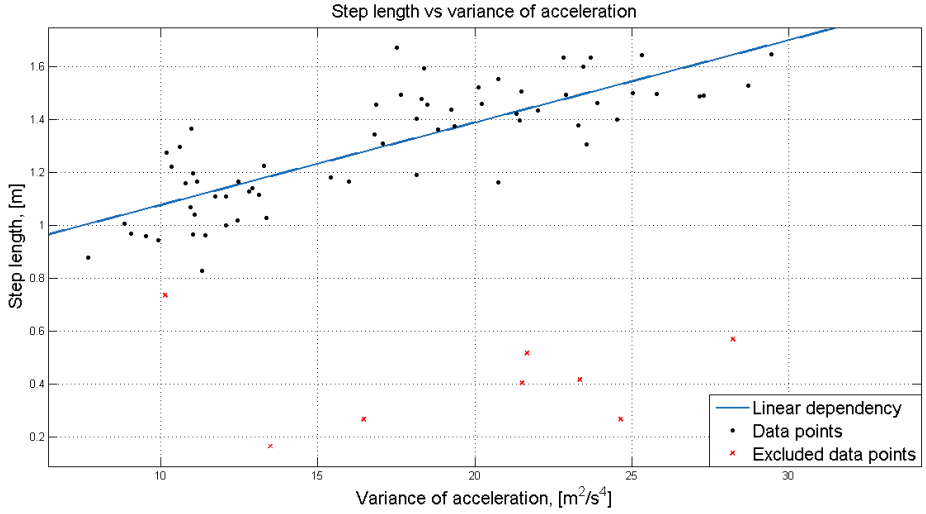


Figure 4: Step length vs variance of acceleration.

Integral of acceleration - Integral of acceleration is just simply a sum of acceleration values during the step, the main difference from variance is that integral has time domain inside, in other words, the longer the step duration is, the higher the value of integral, so integral brings new information for step length estimation. It can be calculated using following equation:

$$A_I = \sum_{n=1}^{N} [a_N - a_g] \tag{17}$$

curve fitting also applied for integral of acceleration:

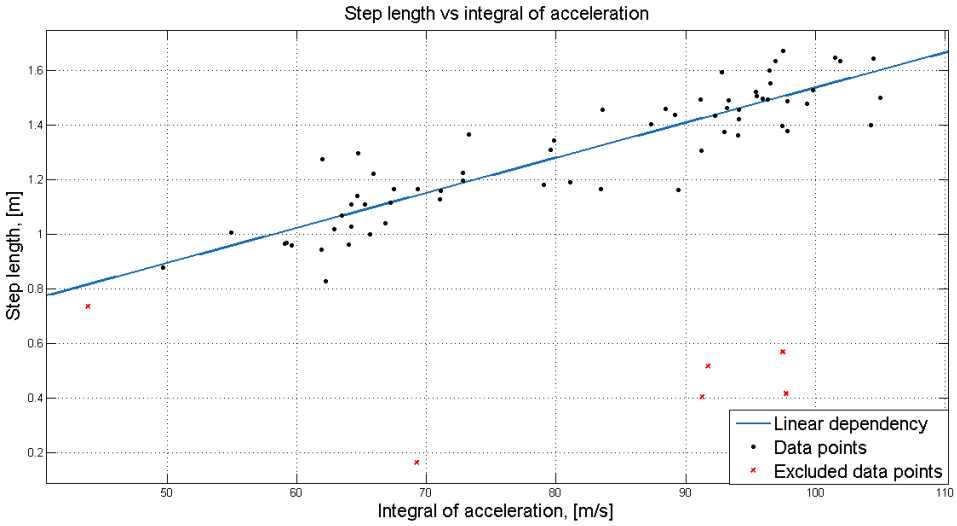


Figure 5: Step length vs integral of acceleration.

Of course it would be sufficient to use only one property to calculate, step length, but step length calculation requires to have some robustness since walking pattern can differ depending from person who is walking. In this case there is two parameters which can represent step length dependency and it possible to find a function with corresponds between these two dependencies.

$$SL = f\{\sigma^2, A_I\} \tag{18}$$

By using previously mentioned curve fitting tool it is possible to find this dependency. In this case linear polynomial is also used ($ax + by + c$).

Curve fitting also provides coefficients which can be used in algorithm to calculate step length knowing the variance of acceleration and integral of acceleration.

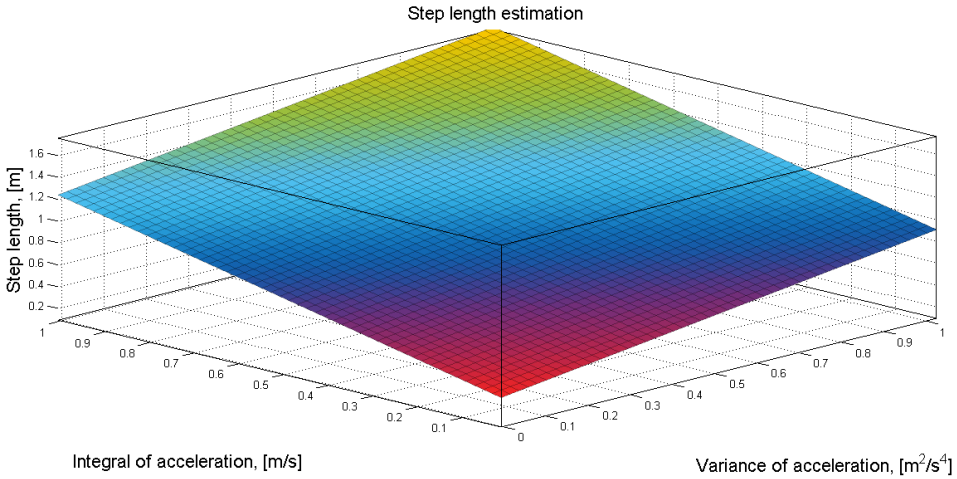


Figure 6: Step length estimation.

5 Position estimation

For position estimation dead reckoning method will be used. In navigation systems dead reckoning is a process when a current position is calculated based on previous position. Based on this method a dynamical model of a system can be derived as:

$$x_n = x_{n-1} + SLcos(\psi) + w_n \tag{19}$$

$$y_n = y_{n-1} + SLsin(\psi) + w_n \tag{20}$$

where x_n, y_n is current position and x_{n-1}, y_{n-1} is the previous positions, accordingly to x and y axes and w_n is the noise of the system

There is no convenient way to remove noise from the model, because it mainly comes from magnetometer, and there is no other source for heading estimation.

The model above allows to represent walking trajectory in 2D space. To more clearly understand the system, flow chart can be used to represent whole precess of it[see figure 7]

6 Results

Experiments were performed in off-line mode, first by recording data with ”Xsense MTw” sensor unit and later processing it in ”Matlab” environment.

Firstly step detection need to be proven. It is an essential part of whole system, if step detection fails, new position will not be calculated, though it is very important to verify that it works correctly. In figure 8 there is data processed by the algorithm and step detection

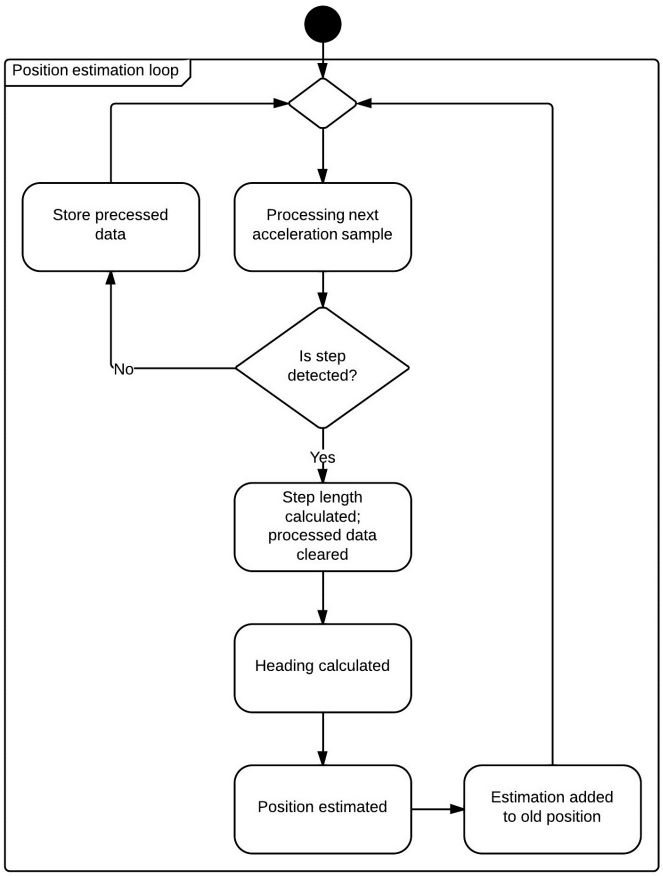


Figure 7: Low power algorithm structure.

trigger is artificially marked. It can be seen, that step detecting has a delay of few samples because of sliding window. But in general case step detection mechanism works fine and further experiments can be carried out.

Finally the full system can be tested. As main purpose of this system is indoor navigation, in figure 9 movement trajectory inside the building is plotted.

Here continues line represent trajectory calculated by a system, and dotted line is approximate true trajectory walked by a human. As it can be seen from figure, calculated trajectory does not fully represent the true trajectory. This problem comes from magnetic disturbances in the building in which experiment was carried out. since there is a lot of electronic equipment and all other sort of material which causes magnetic disturbances, heading estimation is strongly affected by these disturbances, and because it has no implemented way to compensate this disturbances, calculated trajectory is corrupted.

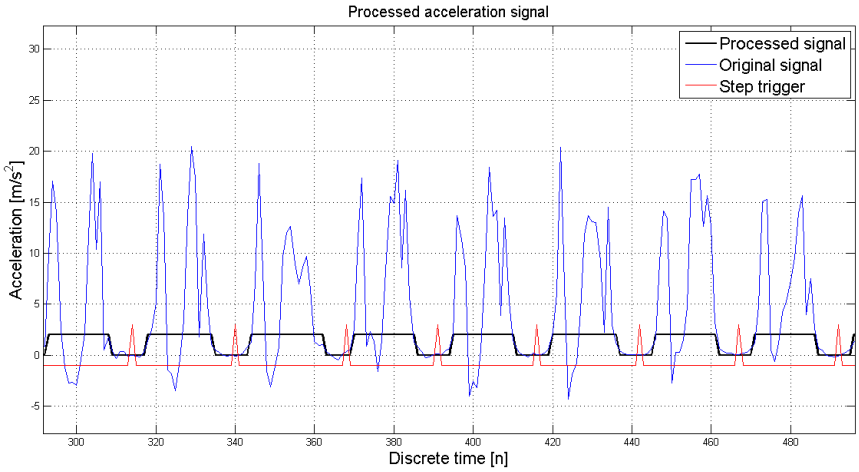


Figure 8: Step detection in acceleration signal.

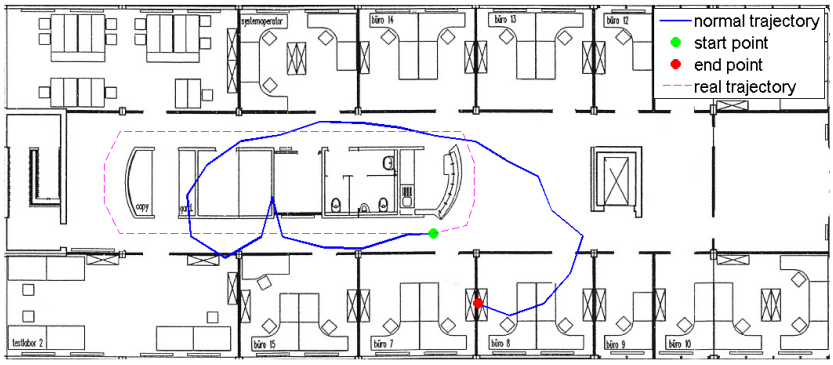


Figure 9: Indoor position estimation representation.

Next, in order to prove that system works sufficient, and main reason of corrupted trajectory is magnetic disturbances, experiments were also performed outside. The resuls can be seen in figure 10:

This time acquired results are comparatively better. Total walked distance is near to 1 km, and the driff between start and end point are about 50 meters. As it can be seen that at one point system starts to drift, this negative effect can be caused by partially bad calibration or by magnetic disturbances. Since it is only development stage of algorithm, further improvement will not be done, and the results will be considered to be good enough to to move to real time system.

Figure 10: Outdoor position estimation representation.

7 Conclusions

Balancing between performance and electrical characteristics is common for a lot of modern electronics, while in this work performance was sacrificed to achieve lowest possible power consumption. Disability to use whole possible hardware and strict computing power allowance led that system created in this work is greatly dependent on external noises and has restrict robustness. Despite this facts system still can be adopted to various application, specially combined with energy harvester (For example: autonomous pedometer). As for the current consumption, at this point main current consumer is communication module. By changing it to less consuming one the current consumption could be reduced dramatically. Moreover goal of this work was to create low power algorithm, and it's current consumption may vary depending on the system it is implemented. Despite quite big overall current consumption, the algorithm itself consumes current in row of hundreds of micro amps, which in this case meets the expectations of low power algorithm. As for future work and improvement on the system, magnetometer calibration technique improvements could bring better performance. Furthermore any possible low power method of heading estimation would add big improvement to trajectory representation. To sum up, even though this project lacks in performance it still can be implemented in some application, or be guidance for other system concerning current consumption.

Acknowledgements

Algorithm development took place in HSG-IMIT institute, Villingen-Schwennengen, Germany, as a part of internship program. I would like to thank my supervisor Vadim Goridko for his huge help making this project come to life and also institute itself for giving me a change to work there and gain a lot of experience. I would also like to thank ERASMUS program which supports students exchange possibility.

References

[AGLA06] Diego Alvarez, Rafael C González, Antonio López, and Juan C Alvarez. Comparison of step length estimators from weareable accelerometer devices. In *Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE*, pages 5964–5967. IEEE, 2006.

[CP06] Seong Yun Cho and Chan Gook Park. MEMS based pedestrian navigation system. *Journal of Navigation*, 59(01):135–153, 2006.

[FG10] Carl Fischer and Hans Gellersen. Location and navigation support for emergency responders: A survey. *IEEE Pervasive Computing*, 9(1):38–47, 2010.

[JBS+10] Jasper Jahn, Ulrich Batzer, Jochen Seitz, Lucila Patino-Studencka, and J Gutiérrez Boronat. Comparison and evaluation of acceleration based step length estimators for handheld devices. In *Indoor Positioning and Indoor Navigation (IPIN), 2010 International Conference on*, pages 1–6. IEEE, 2010.

[KHFM40] Hussam Kloub, Daniel Hoffmann, Bernd Folkmer, and Yiannos Manoli. A micro capacitive vibration Energy harvester for low power electronics. *Work*, 11(25):1, 1740.

[Kon08] Christopher Konvalin. Calculating heading, elevation and bank angle. *Sensors online*, 1:0, 2008.

[MGW+08] Michael Marschollek, Mehmet Goevercin, Klaus-Hendrik Wolf, Bianying Song, Matthias Gietzelt, Reinhold Haux, and Elisabeth Steinhagen-Thiessen. A performance comparison of accelerometry-based step detection algorithms on a large, non-laboratory sample of healthy and mobility-impaired persons. In *Engineering in Medicine and Biology Society, 2008. EMBS 2008. 30th Annual International Conference of the IEEE*, pages 1319–1322. IEEE, 2008.

[RGAJ+12] Michailas Romanovas, Vadim Goridko, Ahmed Al-Jawad, Manuel Schwaab, Martin Traechtler, Lasse Klingbeil, and Yiannos Manoli. A study on indoor pedestrian localization algorithms with foot-mounted sensors. In *Indoor Positioning and Indoor Navigation (IPIN), 2012 International Conference on*, pages 1–10. IEEE, 2012.

[RGK+13] Michailas Romanovas, Vadim Goridko, Lasse Klingbeil, Mohamed Bourouah, Ahmed Al-Jawad, Martin Traechtler, and Yiannos Manoli. Pedestrian Indoor Localization Using Foot Mounted Inertial Sensors in Combination with a Magnetometer, a Barometer and RFID. In *Progress in Location-Based Services*, pages 151–172. Springer, 2013.

[YSS+07] Hong Ying, Carmen Silex, Andreas Schnitzer, Steffen Leonhardt, and Michael Schiek. Automatic step detection in the accelerometer signal. In *4th International Workshop on Wearable and Implantable Body Sensor Networks (BSN 2007)*, pages 80–85. Springer, 2007.

Femtocell deployment: in search of viable Business Models

Gintarė Sukarevičienė, Karolis Žvinys
Vytautas Magnus University,
Department of Applied Informatics, Kaunas,Lithuania and
Vilnius Gediminas Technical University,
Department of Telecommunications Engineering, Vilnius, Lithuania
email: gintare.sukareviciene@gmail.com, karolis.zvinys@vgtu.lt

Abstract: Femtocell (Home NodeB for 3G: HNB, for LTE: HeNB) is a part of heterogeneous mobile networks, which becomes one of the particular promising application domain for so called TV White Spaces. It belongs to self-organizing of low power devices that are typically used to ensure an indoor coverage of different premises: the smaller cells are the more dynamic network you have. Due to this, HNB could be deployed within TV White Spaces without detailed frequencies re-use planning. Overall, the concept of HNB refers to a freedom of installation, increased macro network capacity, femto zone rates and even more.

When deployed, HNB would provide better voice quality, higher data throughput to users, and reduced network deployment expenditures to operators that nowadays become very important issues. Unfortunately, a lot of technical challenges can be faced until the desirable result and performance will be achieved and as of today there is no such the way of benefit, which HNB could give both to operator and subscriber. This refers to the undoubted need of the elaboration of viable Business Models for femtocell deployment.

This paper is focused on non-technical business side of introducing femtocell to the mobile technology by dealing with search of the most attractive way of HNB introduction into the industry that could provide common ground for discussion of the future of HNB, because unplanned deployment of HNB, mobility issues, different types of subscriber groups could cause a headache both for operator and subscriber.
Keywords: Business Model, Cellular networks, Femtocell, Indoor radio communication, Mobile communication, Radio spectrum management.

1 Introduction

Increasing demand of mobile data traffic, customers' expectations, and evolving mobile applications now play a significant role in impelling network operators to look for the new solutions of network availability and quality assurance. The ex-

isting macro network is often too expensive and not always effective because of the suppression of the buildings, while about 50% of the voice calls and 70% of data traffic is generated indoors. Based on this and the analysis of data amount usage in the future [1], it becomes clear that reliable connectivity and indoor services are necessary.

Femtocell (Home NodeB for 3G: HNB, for LTE: HeNB) is the most promising solution to ensure mobile connectivity at home or small business premises. It is small, low-power and low-cost, indoor cellular base station, that is typically designed to operate on Wideband Code Division Multiple Access (WCDMA) network. Today with extant technology, the concept of HNB plus HeNB already exists. It refers to the WCDMA and Long Term Evolution (LTE) supported on the same box [3]. Uncertainty currently exists concerning the way of benefit which HNB could give both to operator and subscriber.

This paper will focus on finding such a way and will be organized as follows: in the second section we introduce the concept of HNB from two different points of view of benefit which HNB could give to operator and subscriber. Moreover, the potential impact of different HNB deployment scenarios is explored in the third section. The fourth section proposes classification of Business Models for HNB deployment and constructs four Business Model configurations based on two value parameters. As a consequence, the third section concludes with analysis on the feasibility to deploy distinct Business Model configuration for the distinct scenarios of HNB deployment. Overall, this paper introduces the concept of HNB in terms of relationships between different stakeholders, such as subscribers and operators.

2 The concept of HNB

HNB is a simple, independent, self-user plug and play implemented device, designed to connect to the service provider's network via broadband [2]. HNB is able to work with all other standards than LTE and WCDMA, such as:

- GSM – a standard of second generation cellular network. Today mostly used for voice calls and data transfer;
- CDMA2000 – a third generation standard of mobile networks, which uses CDMA channel access method;
- TD-SCDMA – a third generation standard of mobile networks;
- WiMAX – a communication standard of wireless networks access. This technology is based on IEEE 802.16 standard;
- Wi-Fi – a wireless technology, mostly used for local data access.

Considering the benefit of HNB from operators' and customers' points of views, it is natural that plenty of advantages both for operators Fig.1 and users Fig.2 exist:

- On one hand, HNB usage opens up wide range of opportunities to operators to free up macro network that leads to increased network capacity. Also HNB lets to extend coverage, reduce cost of macro network expansion and transmission. Due to the minimum of radiation emitted by low power devices, it is easier to register and operate new devices with local regulator authority of communications.
- On the other hand, users can enjoy better signal level indoors, voice quality, and higher data throughputs within area served of HNB. Different services of femto zones become attainable with individual rates of femto zone. Better signal level prolongs handset standby time [4].

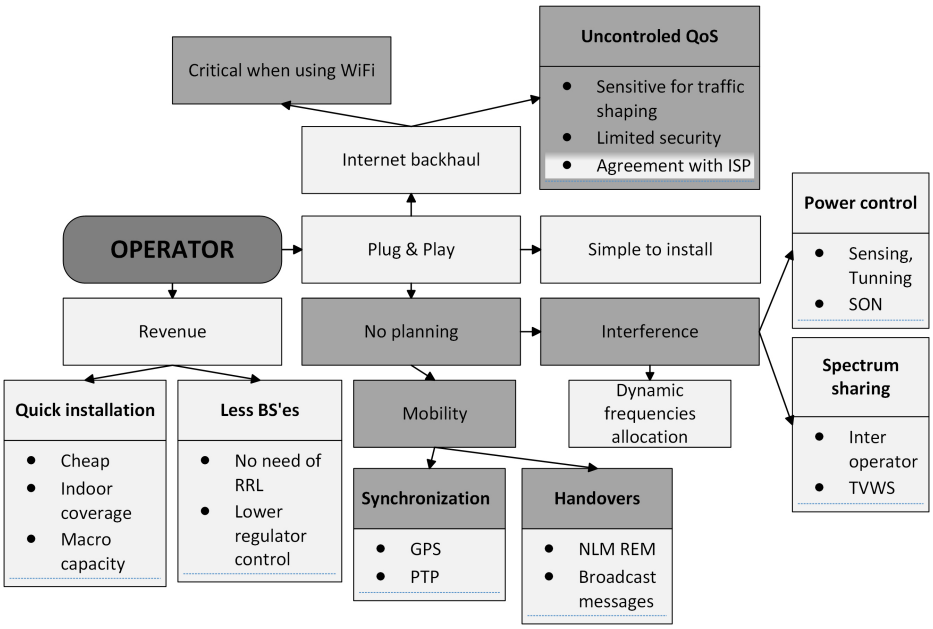


Figure 1: Advantages and disadvantages of HNB from the operator point of view. Note that light grey colour in the figure shows advantages of HNB and dark grey colour refers to disadvantages (RRL here refers to the Remote Radio Links, PTP – Precision Time Protocol, ISP – Internet Service Provider, and SON - Self-Optimizing Networks).

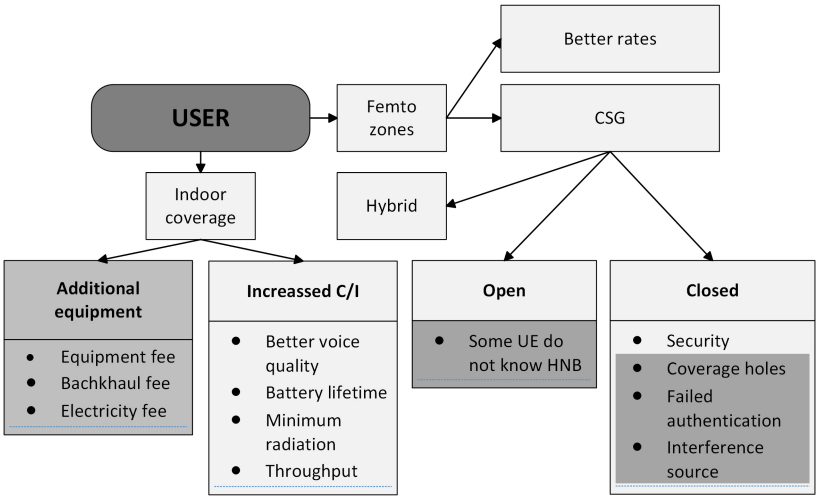


Figure 2: Advantages and disadvantages of HNB from the user point of view. Note that light grey colour in the figure shows advantages of HNB, dark grey colour refers to disadvantages (CSG here refers to the Closed Subscriber Group).

On the contrary to the benefit of HNB, there are some difficulties while achieving all these benefits for the operator Fig.1 and also for the user Fig.2. Besides this, unplanned deployment could cause a lot of issues, when HNB starts to act as interference source. To avoid such disaster it uses interference mitigation methods described on 3GPP [5], [6]. Due to interference avoidance and practically uncontrolled operating, HNB is assigned to Self-Optimizing Networks (SON) category. Before starting to operate each HNB scans its environment and during sensing and tuning phases decides what set of parameters should be used. Persistent measurements collecting and power control ensures that macro and femto networks will operate without any interruptions [7].

One of the key steps in selection process of such a set of parameters is choice of HNB operating frequency, which is most frequently assigned dynamically. Dynamic frequency allocation can be organized using broadcast messages between HNBs. Better choice of frequency is made using measurements from connected User Equipment's (UE's). Such a regulator control of parameters allows achieving high quality services of many functioning HNBs [8]. Also available resources of spectrum are very important, which allow using the channel without harmful interference, for e.g.:

- vacated analogue TV channels, so called – TV White Spaces (TVWS) [9], [10].
- spectrum sharing between operators [11].

From Fig.1, we can conclude that majority of disadvantages from operators' point of view can be solved, while looking from the users' side most of shortcomings could not be changed because they come with a conception of HNB.

3 HNB deployment scenarios

In search of viable Business Models for HNB deployment first step is to identify HNB deployment scenarios. Identification of HNB deployment scenarios below are based on two types of subscriber's groups in terms of possible methods that could be applied according to femto zones configuration as shown in Fig.3.

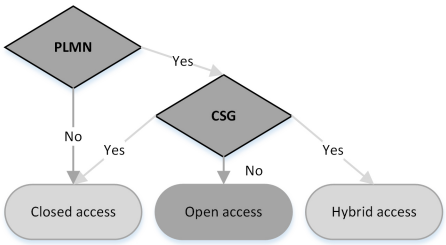


Figure 3: Identification of Business Scenarios for HNB deployment. Note that PLMN refers to the Public Land Mobile Network, CSG – to the Closed Subscriber Group.

From the Fig.3 above it becomes clear that deployment of femto zones can be based on three different scenarios: closed access, open access and hybrid access.

A. Closed access scenario

Closed access refers to HNB services that are not accessible for PLMN users, vice versa it is accessible only for CSGs that are managed by operators. In this case one femtocell can be used to serve just a particular group of users per femtocell: every user have personal list of possible CSGs that are saved in Universal Subscriber Identity Module (USIM). In such scenario operator must manage at least 125 million groups of CSG.

B. Open and hybrid access scenarios

Open and hybrid accesses refer to the possibility to access HNB from any PLMN depending on the agreements of roaming interconnection when one femtocell can serve users with different rights for accessing femto zones. The main difference between these two scenarios is that hybrid access also refers to the possibility to access HNB services to the users of CSG. Note that PLMN users' activity could be restricted in order to ensure good quality of services to the users of CSGs in the case of hybrid scenario.

As a rule, closed and open access models are applied for implementation of new HNB in real networks. Overall, these all three scenarios fundamentally differ from each other depending on relationships between different stakeholders and various parameters that influence these scenarios. Parameters can vary between control and value parameters as shown in Figure 4.

CONTROL PARAMETERS			
Value Network		**Functional Architecture**	
Combination		***Modularity***	
Concentrated	Distributed	Modular	Integrated
Vertical integration		***Distribution of Intelligence***	
Integrated	Disintegrated	Centralized	Distributed
Customer Ownership		***Interoperability***	
Direct	Intermediated	Yes	No
VALUE PARAMETERS			
Financial Model Parameters		**Value Configuration Parameters**	
Cost (Sharing) Model		***Positioning***	
Concentrated	Distributed	Complement	Substitute
Revenue Model		***User Involvement***	
Direct	Indirect	High	Low
Revenue Sharing Model		***Intended Value***	
Yes	No	Price/Quality	Lock-in

Figure 4: Business model matrix.

Based on the Fig.1 and Fig.2, value parameters could be parameters that directly influence deployment of HNB:

A. Revenue Model

On one hand, Revenue Model refers to the operators' point of view. The aim to answer questions on operator's revenue became very important as operators and manufacturers have no other choices as to look for new effective spectrum utilization option due to their spectrum scarcity, while demand for mobile data is increasing. Unfortunately, the coding of the channel, cognitive transmissions, multiple-input and multiple-output (MIMO) have already reached their theoretical limits. These left the operators with no option than to revise existing network topologies which are moving towards heterogeneous network approach that leads to the Revenue Models' changes. But how then business should gain benefit?

B. User Involvement

On the other hand, User Involvement refers to the subscribers' point of view. The most essential problem here is the cost of HNB, because nowadays in markets where the distribution and supply of HNB are more visible HNB remains rather expensive solution. This is because HNB equipment fee is included into monthly cost of services. This fee increases the total cost 20-40%. Due to this, operators and services providers apply various methods in order to keep their subscribers, for. e.g.: free calls, free data flows within HNB area. But is here a way to make

total cost of HNB solution to users as low as possible?

In the further section for the classification of Business Models for HNB deployment these two value parameters (Revenue Model and User Involvement) are used. As a rule, the more parameters are used to perform classification, the more detailed classes of Business Models could forth come.

4 Classification of Business Models

Here can be plenty of different Business Models for HNB. In order to get better view of all possible Business Models for HNB, they all could be grouped into various classes depending on the parameters that influence them.

As shown in Fig.5, we have distinguished four groups of Business Models for HNB depending on the value parameters (see Figure 4 in Section III).

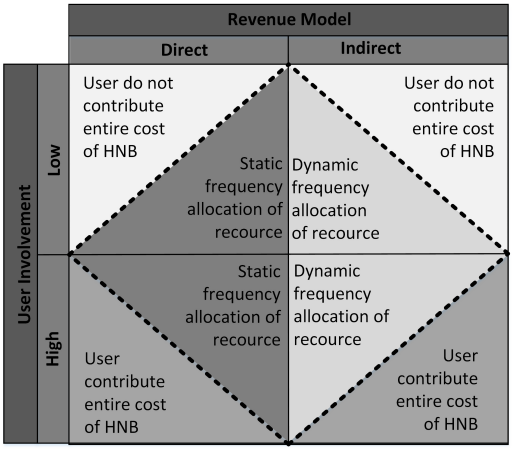


Figure 5: Identification of Business Models groups. Note that power of HNB management can be centralized or distributed. Note that static frequency allocation is not possible in case of high speed packet access (HSPA) by using only one carrier in the system. Dynamic frequency allocation refers to the steady information about frequencies resources exchange between femto and macro networks. Thus, the easiest way to allocate frequency resources is to split them between different levels but this would be not efficient due to different workloads between femto and macro cells.

A. Direct and indirect Business Models

Direct and indirect Business Models represent the influence of the first value parameter (Revenue Model). Direct Business Model refers to the solution when HNB UE maximum uplink transmit (UL Tx) power is regulated in order to manage

interferences caused directly by the UE(UL) to NodeB of macro network that is maintained by HNB. In this case, UL Tx power is managed on the basis of the measurements collected by UE while UE is connected to HNB. Accordingly, indirect Business Model refers to the solution when interference to HNB downlink (DL) is managed from macro network side.

B. High and Low user' Involvement Business Models

Business Models that ensure lower and higher total cost of HNB for subscribers according to the influence of second parameter (User Involvement).

Business Models for HNB must show the best solution for frequency allocation for HNB deployment. Herewith such a Business Model must also be understandable for governmental and industrial agencies and for operators in order to commercialize HNB technology in the ways that will allow capturing value from their investments to the technology. Thus, it becomes very important to analyse them in order to find the best solution to be implemented in the future.

In order to analyse proposed Business Model classes, based on the chosen value parameters it is possible to distinguish between four Business Model configurations. The latter Business Model configurations can be understandable as more detailed Business Models classifications that shows who plays the main role within the appropriate Business Model group for HNB:

- *Operator-based configuration* – the main role is played by HNB operator that manages the coverage of femto network;
- *Outsource-based configuration* – the main role is played by the third party that is aided by HNB operator who develops and operates HNB network;
- *User-based configuration* – the main role is played by the UE that allows to control the level of the interference and ensure optimum coverage of femto cell;
- *Broker-based configuration* – the main role is aided by broker at the same time ensuring high user involvement.

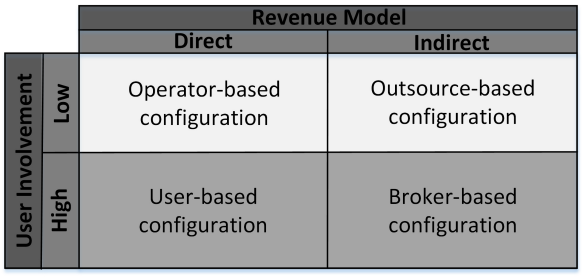


Figure 6: Business Model for HNB matrix based on two value parameters

Thus, these Business Models configurations for HNB deployment (as shown in Fig.6) can be matched with scenarios proposed in section III (as shown in Fig.3). Note that within each scenario not all Business Model configurations are possible (Fig.7).

- Within closed access scenario only two configurations (operator and user-based) seems to be possible to be implemented in the future;
- Within open access scenario also two configurations (outsource and broker-based) can be matched;
- Within hybrid access scenario all proposed configurations are likely to be applied.

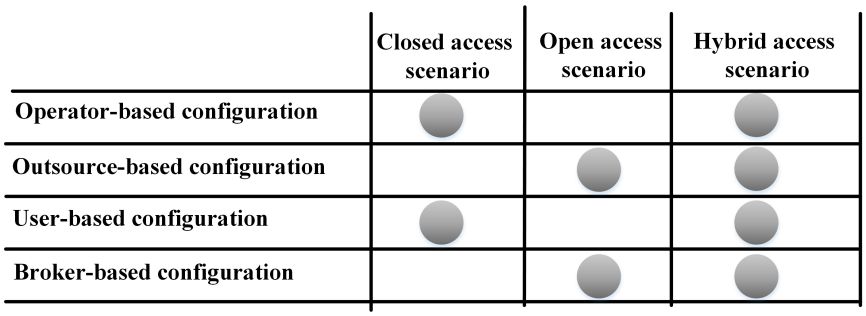


Figure 7: HNB deployment scenarios and their possible Business Model configurations.

Further evaluation of the viability of each Business Model configuration is mandatory in order to choose the best solution that would help HNB to be implemented in the correct way in the future.

5 Conclusions

HNB – modern solution for mobile communication network that in principle changes the way of contemporary mobile network deployment. HNB offers plenty of new business opportunities, such as: Small cell as a service (ScAAS), cognitive femto access points (FAPs), solution of HNB plus WiFi, and much more. For the user it could create secure connection to the network in the weak signal areas, for the operator – to ensure network capacity and coverage.

In this paper we analyzed and proposed different Scenarios and possible Business Models for HNB, which were classified into four classes and four separate Business Models configurations. Each configuration was matched with appropriate HNB

deployment scenario. This could be the starting point for further researches in order to identify the optimal Business Model within each scenario, based on the potential viability of each model configuration. Besides this, it would allow to choose the best solution to be implemented in the future for the use of HNB.

Acknowledgements

This work was supported in part of the COST Action IC0905 TERRA "Techno-Economic regulatory framework for radio spectrum Access for Cognitive Radio/Software Defined Radio".

References

[1] Ericsson, "Traffic and market report: on the pulse of the networked society", Stockholm: Ericsson AB, 2012, pp. 7.

[2] K. Elleithy, V. Rao, "Femto Cells: Current Status and Future Directions", Int. Journal of Next-Gedneration Networks, vol. 3, No.1, March 2011.

[3] NTT DOCOMO, Inc, "DOCOMO Develops World's First Small-cell Base Station for 3G and LTE: Details of New Dual-mode Femtocell", Press Release, Nov. 16, 2012.

[4] Qualcomm, "Femtocells", April 2011, pp. 29.

[5] 3GPP TS 25.467, "UTRAN architecture for 3G Home Node B (HNB), Stage 2", France, 2012, pp 61.

[6] M. Yavuz et al., "Interference Management and Performance Analysis of UMTS/HSPA+ Femtocells", IEEE Communications magazine Femtocell Wireless Communications, Sep. 2009 [online]. Available: www.qualcomm.com/media/documents/files/interference-management-and-performance-analysis-of-umts-hspa-femtocells.pdf

[7] J. G. Andrews, H. Claussen, M. Dohler, S. Rangan, M. C. Reed, "Femtocells: Past, Present, and Future" [online]. Available:http://users.ece.utexas.edu/ jandrews/pubs/JSAC_FemtoSurvey.pdf

[8] D. Lopez-Peres, A. Ladanyi, A. Juttner, J. Zhang, "OFDMA femtocells: A self-organizing approach for frequency assignment", UK Luton: University of Bedfordshire [online]. Available:http://www.cs.elte.hu/ alpar/publications/proc/ 2009PIMRCSelforganization.pdf

[9] Qualcomm, "The Wireless Evolution", 2011, pp. 43.

[10] C. F. Silva, H. Alves, A. Gomes, "Extension of LTE Operational Mode over TV White Spaces", in 2011 Proc. Future Network and MobileSummit [online]. Available:http://www.ict-cogeu.eu/pdf/ publications/Y2/FUNEMS_2011_COGEU_paper_n2.pdf

[11] M. M. Buddhikot, I. Kennedy, F. Mullany, H. Viswanathan, "Ultra-Briadband Femtocells via Opportunistic Reuse of Multi-Operator and Multi-Service Spectrum", Bell Labs Technical Journal 13(4), pp. 129-144, 2009 [online]. Available:http://www.bell-labs.com/user/mbuddhikot/psdocs/cogfemto/BLTJ134_08_129-144-photoready.pdf

[12] P. Ballon, "Business Modelling Revisited: The Configuration of Control and Value", The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media, 9(5):6-19, 2007.

Pseudo-random Number Generators Based on Multiplicative Elliptic Curves

Omar Reyad[1,2], Zbigniew Kotulski[2]
[1]Faculty of Science, Sohag University, Egypt
[2]Faculty of Electronics and Information Technology,
Warsaw University of Technology, Poland
email: ormak4@yahoo.com, zkotulsk@tele.pw.edu.pl

Abstract: Pseudo-random number generators (PRNG) play main important role in many security and cryptographic applications which require the output to be unpredictable and this is directly related to the quality of the generated random sequences. The design of such random sequences generators is not an easy task. Elliptic Curve Cryptography (ECC) is a relatively recent branch of cryptography which is based on the arithmetic on elliptic curves and security of the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP). Elliptic curve cryptographic schemes are public-key mechanisms that provide encryption, digital signature and key exchange capabilities. Elliptic curve algorithms are also applied to generation of sequences of pseudo-random numbers. In the present work, we propose a method of generating sequences based on multiplication of points of elliptic curves over finite fields which is driven by a chaotic map. The random sequence generated using our method has been subjected to a battery of statistical tests developed by National Institute of Standards and Technology (NIST). The results show that the proposed generator can generate pseudo-random numbers effectively as standard generators with good randomness properties makes it suitable for both classical and elliptic curve cryptography.

1 Introduction

In the recent past, elliptic curve cryptography (ECC) has received great interest from cryptographers, mathematicians, and computer scientists around the world [Certicom, M93]. The primary reason for this is its high security over existing public key cryptographic algorithms. The best algorithm known for solving the underlying mathematical problem of ECC, referred to as the elliptic curve discrete logarithm problem (ECDLP), takes full exponential time. On the contrary, sub-exponential time algorithms are known for tackling the integer factorization and the discrete logarithm problems that RSA and DSA are relied on [CDELMZ96]. This implies that the algorithms for solving the elliptic curve discrete logarithm problem become infeasible much more rapidly as the problem size increases than those algorithms for tackling the integer factorization and the discrete logarithm problems. For this reason, ECC offers a security level equivalent to RSA and DSA while using a far smaller key size.

On the other hand, the security of most cryptographic systems depends upon the generation of unpredictable quantities that must be of sufficient size and randomness. This implies

that we usually need to implement a random number generator in a cryptographic system.

However, sources of truly random integers are hard to use in practice. It is therefore common to search for pseudo-random number generators. Roughly speaking, a pseudo-random source may not be distinguished from a truly random source by any polynomial time algorithm. Several pseudo-random number generators have been proposed which are using the form of elliptic curves such as [JJV07]. Since then, different approaches for extracting pseudo randomness from elliptic curves which referred to as Elliptic Curve Pseudo-Random Number Generator (ECPRNG) have been proposed by [GBS00].

As we already remarked, the great advantage of elliptic curve cryptography is operating over small-size finite fields (comparing other public-key cryptosystems). However, in case of pseudo-random numbers generator small finite fields imply short period of a generator. Therefore, to increase the period of a generator working on an elliptic curve we propose to combine it with a chaotic map.

The idea of application of chaotic maps for constructing cryptosystems have been presented in [HNSM91] where the authors proposed using chaotic maps' parameters as a secret key. Recent years such cryptosystems were extensively studied [KL11] with large variety of particular algorithms and applications. Among them Chaotic Pseudo-Random Number Generators (CPRNG) initiated in [KT97] found many effective implementations since their period is (by theory) infinite.

In this paper we propose a new method of generating sequences of pseudorandom points on elliptic curves over finite fields which is driven by a chaotic map. Such a construction increases randomness of the sequence generated and makes its period (theoretically) infinite since it combines positive properties of an ECPRNG and a CPRNG [RK15, RK14]. After transformation of the points into binary numbers it can be used for any cryptographic applications.

The organization of the rest of the paper is as follows. In Section 2, the construction of CPRNG and the background of elliptic curves over finite fields are discussed in Subsections 2.1, 2.2 respectively. The proposed random number generator will be described in Section 3. The test results are reported in Section 4. In Section 5, discussions and conclusions are made.

2 Preliminaries

2.1 Construction of CPRNG

Consider the following dynamical system defined as a pair (S, Φ), where S is the state space (usually metric space) and $(\Phi : S \to S)$ is a measurable map which is the generator of the semigroup of iterations [CFS82]. The trajectory starting from the initial state s_0 is the sequence $(s_0)_{i=0}^{\infty}$ of elements of S obtained by iteration

$$s_{i+1} = \Phi(s_i), i = 0, 1, 2, ... \tag{1}$$

Assume that μ is a normalized invariant measure of the system, equivalent to a Lebesgue measure. The idea of construction of CPRNG is to divide the state space S, $\mu(S) = 1$, into two disjoint parts S_0, S_1 such that $\mu(S_0) = \mu(S_1) = 1/2$. As a seed we shall consider an initial point $s \in S' \subseteq S$, where S' is the set of acceptable seeds (for most systems, $\mu(S') = 1$). To obtain a pseudo-random sequence of bits we observe the iterations of the system governed by the map Φ starting from s, i.e., the sequence $s_i := \Phi^i(s)$. We assume that the i-th bit $b_i(s)$ of the generated pseudo-random sequence is equal to "0" if $s_i \in S_0$, and is equal to "1" otherwise, so as a result of iterations we obtain the infinite sequence of bits $G(s)$. Finally, we obtain the map

$$G : S' \to \prod_{i=1}^{\infty} \{0, 1\}, \tag{2}$$

such that

$$G(s) = \{b_i(s)\}_{i=1,2,...} = \{b_1(s), b_2(s), ...\}, \tag{3}$$

and where $\prod_{i=1}^{\infty} \{0, 1\}$ is the Cartesian product of the infinite number of the two-element set $\{0, 1\}$.

Moreover, theoretically the period of such a CPRNG is infinite, since it is iterated over the infinite state space S.

In many practical applications for constructing CPRNG we assume that $S = [0,\ 1]$ is the interval, $S_0 = [0\ ,\ 0.5]$, $S_1 = (0.5\ ,\ 1]$ are two subsets of the measure equal 0.5 and $\Phi : [0,\ 1] \to [0,\ 1]$ is a chaotic map with positive Lyapunov exponent λ.

2.2 Elliptic Curves over Finite Fields

For a prime p let us denote by F_p is the finite field of p elements. Let E be an elliptic curve over F_p, $p > 3$, given by an affine Weierstrass equation of the form

$$E : y^2 = x^3 + ax + b \tag{4}$$

with coefficients $a, b \in F_p$, such that $4a^3 + 27b^2 \neq 0$. We recall that the set $E(F_p)$ of F_p-rational points on any elliptic curve E forms an Abelian group (with a point at infinity denoted by O as the neutral element) and the cardinality of this group satisfies the Hasse-Weil bound

$$|\#E(F_p) - p - 1| \leq 2\sqrt{p} \tag{5}$$

Point addition and point doubling are the basic EC operations. Point multiplication on EC requires scalar multiplication operation. Let P be a point with the coordinates x, y on an

EC, and one needs to compute kP, where k is a positive integer. This scalar multiplication can be done by a series of doubling and addition of P.

Let us start with $P = (x_1, y_1)$ where $P \neq -P$. To determine $2P = (x_3, y_3)$, P is doubled, use the following equation, which is a tangent to the curve at point P.

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

and

$$y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$$

To determine $3P$, addition of points P and $2P$ is used, treating $2P = Q$. Here, P has coordinates $P = (x_1, y_1)$. $Q = 2P$ has coordinates $Q = (x_2, y_2)$, where $P \neq \pm Q$. Then $P + Q = (x_3, y_3)$, where

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

and

$$y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

Therefore, doubling and addition are applied depending on a sequence of operations determined for k. Every point (x_3, y_3) evaluated by doubling or addition is an affine point (points on the EC). For this and some other general properties of elliptic curves see [BSS99, S95].

3 The Proposed Random Number Generator

For a given point $G \in E(F_p)$ and an integer $e \geq 2$, we can define the following sequence:

$$U_i = e^{i(1+b_i)}G = \begin{cases} e^i G & \text{if} \quad b_i = 0 \\ e^{2i} G & \text{if} \quad b_i = 1 \end{cases}, i = 1, 2, ... \tag{6}$$

where $U_0 \in E(F_p)$ is the "initial value" and b_i is the random bits generated by the chaotic map Φ

$$b_i = \begin{cases} 0 & \text{if} \quad \Phi^i(s) \in S_0 \\ 1 & \text{if} \quad \Phi^i(s) \in S_1 \end{cases}, i = 1, 2, ... \tag{7}$$

Using EC point sequence U_i and by converting the x, y coordinates of each point $U_i(x, y)$ into binary format we can obtain the bit sequence B_i by applying the following map

$$B_i = U_i(x, y) = \begin{cases} U_{2x2}(x, y) \\ U_{3x3}(x, y) \end{cases}$$

This map takes the two right-most bits from x coordinate and the two right-most bits from y coordinate which denoted $U_{2x2}(x, y)$. Analogously, by taking the three right-most bits from x coordinate and y coordinate which denoted $U_{3x3}(x, y)$ we can obtain another bit sequence and we skip the infinity points also.

Example Consider the curve $E : y^2 = x^3 + x + 4$ over F_{11} . This curve has order 9 and is cyclic. Here $p = 11$. Let $G = (2, 6)$ be a point on E. The EC points U, together with the bit sequence B in the two cases, are listed in Table 1. Note, we skip the Infinity points I.

Table 1: An example of transforming EC points into binary sequences

i	$U_i(x, y)$	$U_i(x, y)_2$	$B_i(U_i)_{2x2}$	$B_i(U_i)_{3x3}$
1	(9, 7)	(1001,0111)	(01,11)	(001,111)
2	(0, 2)	(0000,0010)	(00,10)	(000,010)
3	(2, 6)	(0010,0110)	(10,10)	(010,110)
4	(9, 7)	(1001,0111)	(01,11)	(001,111)
5	(0, 2)	(0000,0010)	(00,10)	(000,010)
6	(2, 6)	(0010,0110)	(10,10)	(010,110)
7	(I, I)	(—-,—-)	(–,–)	(—,—)
8	(9, 7)	(1001,0111)	(01,11)	(001,111)
9	(2, 5)	(0010,0101)	(10,01)	(010,101)

So, the output binary sequences will be
B_{2x2} = 011100101010011100101010011111001...
and
B_{3x3} = 001111000010010110001111000010 01...

4 Test Results

Extensive statistical testing was used to assess or estimate the quality of PRNG. Test suites developed for this purpose may be found in [FIPS00, K81]. From these tests we selected 5 which taken together verify random properties of sequences generated. They are:

1. The monobit test (in Tables 2 - 7 named *Frequency Test*), which verifies if the number of "1" bits in the sequence lies within specified limits.

2. The cumulative sums test, which determines whether the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected behavior of that cumulative sum for random sequences. The test has two modes, which are either forward through the sequence or backward through the sequence, named in the Tables *C.Sum F.* and *C.Sum R.*, respectively.

3. The runs test (*Runs Test* in the Tables) checking whether the number of runs (the test is carried out for runs of zeros and runs of ones) of length 1, 2, 3, 4 and 5 as well as the number of runs which are longer than 5, each lies within specified limits.

4. The long run test (*L. Runs Test*) confirming that in the tested sequence there must be no run of length equal to or greater than 34 bits.

5. The discrete Fourier transform test (*DFT*) detecting the periodic features in the tested sequence that would indicate a deviation from the assumption of randomness.

Thus, in these 5 tests, the monobit test verifies if globally the binary distribution is symmetric, the cumulative sums tests check if the sequence is symmetrically growing during bits generation, the runs test and the long run test confirm bits independence and the discrete Fourier transform test allows detecting periodic behavior of the binary sequence generated. Additional motivation for such a choice of such a set of 5 tests (from all 15 tests proposed in the document SP800-22b [RSN01]) is that they can be applied for binary sequences of different size, also very short ones. In our investigations we used sequences of 100, 200, 500, 1000, 2000 and 5000 bits for the generators constructed on EC over small finite field.

The statistical tests made in this paper were on the significance level α equal to 0.01, so the tests are passing if P-value ≥ 0.01,. Moreover, the larger the P-value is, the better the pseudorandom property the generator is.

To investigate the effect of chaotic modulation of the multiplicative ECPRNG we considered the elliptic curve over p= 229 finite fields. First, we tested random properties of the binary sequences governed by the two following maps:

the Logistic Map [PR95]:

$$s_{i+1} = \Phi(s_i) = 4 \cdot s_i (1 - s_i), \tag{8}$$

for the state space $S = [0, 1]$ and $S_0 = [0, 0.5]$, $S_1 = (0.5, 1]$, and the Chebyshev Map [LLP04]:

$$s_{i+1} = \Phi(s_i) = \cos\left(4 \cos^{-1}(s_i)\right), \tag{9}$$

for the state space $S = [-1, 1]$ and $S_0 = [-1, 0]$, $S_1 = (0, 1]$.

In the experiments we used the following elliptic curve:

$$E_1 : y^2 = x^3 + x + 4 \tag{10}$$

over F_{229}

Results of testing the sequences generated are presented in Tables 2 - 7. In Table 2 are presented results for the multiplicative ECPRNG on the curve E for the case EC_{2x2} without chaotic modulation. As it is expected, the generator works correctly for short binary sequences (500 bits) due to its periodicity, what is indicated by the DFT Test.

Table 2: ECPRNG without chaotic modulation. P-values for the case $EC_{2x2}, p = 229$

Test name	Case 1 100 bits	Case 2 200 bits	Case 3 500 bits	Case 4 1000 bits	Case 5 2000 bits
Frequency	1.000000	0.479500	0.858028	0.899343	0.928730
C. Sum F.	0.990843	0.834306	0.727622	0.941731	0.997333
C. Sum R.	0.990843	0.704309	0.563698	0.850473	0.982440
Runs	0.230139	0.060309	0.282459	0.113725	0.028413
L. Runs	1.000000	1.000000	1.000000	1.000000	1.000000
DFT	0.745603	1.000000	0.468160	**0.001027**	**0.000000**

Table 3: ECPRNG modulated with the Logistic map. P-values for the case $EC_{2x2}, p = 229$

Test name	Case 1 100 bits	Case 2 200 bits	Case 3 500 bits	Case 4 1000 bits	Case 5 2000 bits
Frequency	0.548506	0.479500	0.654721	0.949571	0.654721
C. Sum F.	0.958638	0.514421	0.885595	0.922381	0.867899
C. Sum R.	0.722386	0.704309	0.685633	0.958243	0.902311
Runs	0.714876	0.644963	0.585190	0.164063	0.048563
L. Runs	1.000000	1.000000	1.000000	1.000000	1.000000
DFT	0.745603	0.358795	0.468160	0.538167	0.146793

Table 4: ECPRNG modulated with the Chebyshev map. P-values for the case $EC_{2x2}, p = 229$

Test name	Case 1 100 bits	Case 2 200 bits	Case 3 500 bits	Case 4 1000 bits	Case 5 2000 bits
Frequency	0.548506	0.777297	0.928730	0.849515	0.754243
C. Sum F.	0.722386	0.939470	0.999373	0.982178	0.992221
C. Sum R.	0.814758	0.704309	0.992221	0.994708	0.987998
Runs	0.149531	0.118308	0.128283	0.099850	0.019922
L. Runs	1.000000	1.000000	1.000000	1.000000	1.000000
DFT	0.330390	0.646355	0.468160	0.681519	0.383988

Including the chaotic PRNG enables generating correctly longer sequences: 2000 bits for the Logistic Map (Table 3) and Chebyshev Map (Table 4). Analogously, for the larger

sequence EC_{3x3} the non-disturbed ECPRNG gave a correct result till 1000 bits generated, as it is seen from Table 5. The generators driven by the two chaotic maps (8) and (9) give much correct pseudo-random bits (5000 bits), see Tables 6 and 7. For 10000 and more bits the DFT test indicates the generators' periodicity.

Table 5: ECPRNG without chaotic modulation. P-values for the case $EC_{3x3}, p = 229$

Test name	Case 1 100 bits	Case 2 200 bits	Case 3 500 bits	Case 4 1000 bits	Case 5 2000 bits	Case 6 5000 bits
Frequency	0.548506	0.777297	1.000000	0.899343	0.964329	0.932378
C. Sum F.	0.540731	0.834306	0.563698	0.850473	0.982440	0.999972
C. Sum R.	0.814758	0.991720	0.563698	0.941731	0.966907	0.998656
Runs	0.661694	0.023250	0.179712	0.087606	0.081128	0.011822
L. Runs	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000
DFT	0.745603	0.358795	0.884636	0.013803	**0.000001**	**0.000000**

Table 6: ECPRNG modulated with the Logistic map. P-values for the case $EC_{3x3}, p = 229$

Test name	Case 1 100 bits	Case 2 200 bits	Case 3 500 bits	Case 4 1000 bits	Case 5 2000 bits	Case 6 5000 bits
Frequency	0.548506	0.777297	0.325179	0.704336	0.928730	0.350623
C. Sum F.	0.958638	0.998656	0.644038	0.823133	0.975431	0.514421
C. Sum R.	0.540731	0.892023	0.304777	0.900481	0.992221	0.396008
Runs	0.065383	0.046994	0.226899	0.280194	0.194596	0.010963
L. Runs	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000
DFT	0.330390	0.646355	0.309788	0.837419	0.561658	0.408863

Table 7: ECPRNG modulated with the Chebyshev map. P-values for the case $EC_{3x3}, p = 229$

Test name	Case 1 100 bits	Case 2 200 bits	Case 3 500 bits	Case 4 1000 bits	Case 5 2000 bits	Case 6 5000 bits
Frequency	0.841481	0.887537	0.788447	0.800282	0.531250	0.820988
C. Sum F.	0.897326	0.991720	0.885595	0.971736	0.769421	0.796506
C. Sum R.	0.990843	0.939470	0.966907	0.994708	0.830116	0.961431
Runs	0.160152	0.033758	0.369305	0.446646	0.259734	0.011801
L. Runs	1.000000	1.000000	1.000000	1.000000	1.000000	1.000000
DFT	0.330390	0.066457	0.663355	0.304902	0.468160	0.581909

5 Conclusions

In this paper we proposed a new construction of a pseudorandom number generator which uses both elliptic curves and chaotic maps for bit streams generation. As our experiments presented in Section 4 shown such a combination gave us the construction with positive properties being resultant properties of the two components. Comparing purely EC-based pseudorandom number generator, our construction has longer period for a fixed size of the finite field F_p where the EC lives. Thus, we can use smaller fields (with less computational complexity of arithmetic calculations) to obtain a bitstream of a fixed length.

The experiments presented in this paper confirm that our theoretical assumptions concerning the new construction of the PRNG are satisfied. However, to optimize the procedures of generation further extensive studies must be performed.

Acknowledgements

The authors gratefully acknowledge the Egyptian Ministry of Higher Education and Scientific Research for financially supporting this research grant.

References

[M93] A. Menezes. Elliptic Curve Public Key Cryptosystems. Kluwer Academic, (1993).

[Certicom] Certicom Corp. http: //www. certicom. com/.

[CDELMZ96] J. Crowie, B. Dodson, R. Elkenbracht-Huizing, A. Lenstras, P. Montgomery, J. Zayer. A world wide number field sieve factoring record: On to 512 bits. In Advances in Cryptology- ASIACRYPT '96, pp. 382-394, Springer-Verlag, (1996).

[JJV07] D. Jao, D. Jetchev, R. Venkatesan. On the bits of elliptic curve diffie-hellman keys. In: Srinathan, K., Rangan, C.P., Yung, M. (eds.) INDOCRYPT 2007. LNCS, vol. 4859, pp. 33–47. Springer, Heidelberg (2007)

[GBS00] G. Gong, T.A. Berson, D.R. Stinson. Elliptic curve pseudorandom sequence generators. Selected areas in cryptography (Kingston, ON, 1999), pages 34-48. Springer, Berlin, 2000

[HNSM91] T. Habutsu, Y. Nishio, I. Sasase, S. Mori. A secret key cryptosystem by iterating a chaotic map. Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp.127-140, Springer 1991.

[KL11] L. Kocarev, Sh. Lian, (Eds.). Chaos-based Cryptography. Theory, Algorithms and Applications. Series: Studies in Computational Intelligence, Vol. 354, Springer 2011.

[KT97] T. Kohda, A. Tsuneda. Statistic of chaotic binary sequences. IEEE Transactions on Information Theory 43, no.1: 104-112. 1997.

[RK15] O. Reyad, Z. Kotulski. On Pseudo-random Number Generators Using Elliptic Curves and Chaotic Systems. J. Applied Mathematics and Information Sciences, vol.9, no.1, 2015.

[RK14] O. Reyad, Z. Kotulski. Statistical Analysis of the Chaos-Driven Elliptic Curve Pseudo-random Number Generators. CCIS, vol.448, pp.38-48, Springer Berlin Heidelberg, 2014.

[CFS82] L.P. Cornfeld, S. V. Fomin, and Ya.G. Sinai. Ergodic Theory. Springer-Verlag, Berlin 1982.

[S95] J.H. Silverman. The arithmetic of elliptic curves. Springer-Verlag, Berlin, 1995.

[BSS99] I. Blake, G. Seroussi, N. Smart. Elliptic curves in cryptography. London Math. Soc., Lecture Note Series, 265, Cambridge Univ. Press, 1999.

[FIPS00] FIPS 140-2. Security Requirements for Cryptographic Modules. NIST, 2000.

[K81] D.E. Knuth. The Art of Computer Programming - Seminumerical Algorithms. vol. 2, Addison-Wesley, Reading, 1981.

[RSN01] A. Rukhin, J. Soto, J. Nechvatal et.al.. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. NIST Special Publication 800-22 with revisions, May 15, 2001.

[PR95] S.C. Phatak, S.S. Rao. Logistic map: A possible random-number generator. Physical Review E, vol.51, no.4, pp.3670-3678, 1995.

[LLP04] X.F. Liao, X.M. Li, J. Peng, et al. A digital secure image communication scheme based on the chaotic Chebyshev map. Int. J. Commun. Syst., vol.17, no.5, pp.437-445, 2004.

Information Delivery Optimization in a Lecture

Robin Nicolay, Clemens H. Cap
University of Rostock
email: {Robin.Nicolay,Clemens.Cap}@uni-rostock.de

1 Introduction

More and more applications use mobile devices to increase the number of simultaneously available communication channels. This increased number of channels allow a parallel delivery of auxiliary content. Examples are TV-shows which augment their program through mobile apps and websites [Fit13]. While reviewing this evolution, we noticed that provided additional content has to match the capacity of a user's perception. In our work we describe concepts and ideas how to extend existing multi-display environments in a presentation scenario with private mobile devices to improve the process of information delivery.

The question of how to efficiently integrate multi-display environments into our daily life has been a research topic for some time. Great achievements have been made in the the area of presentation scenarios and interactions with presentations in multi-display environments [ZL04, RLS11, RLSS12, Sey13, SBSM13].

However, recent developments in the area of mobile devices present new requirements and challenge existing approaches. Current benchmarks state that CPU power of mobile devices doubles every year [Pri14b, Pri14a]. New sensor hardware enables mobile devices to sense user's activities and surroundings [KXAA13]. New types of devices such as augmentation glasses, smart watches or even rings are currently under development. These devices provide more and more displays, sensors, and interaction capabilities.

2 Methods and Materials

Our work is part of MuSAMA[1] which is a research project based on the hypothesis that in an everyday environment ubiquitous intelligent machines can be enabled to interact and cooperate with each other in a spontaneous and autonomous way. This cooperation should enable a group of devices to identify and achieve the user's goal [Kir14].

In this context, we focus on the question how this technical development can be used to increase the perception capacity. As initial step of our work, we reviewed a scenario which

[1] Multimodal Smart Appliance Ensembles for Mobile Applications

includes high demands on content delivery and identified gaps we want to improve.

Our scenario is a typical lecture setting with a big audience of more than 30 people. One or more lecturers talk to a audience consisting of students with private mobile devices (See [Han13] for recent statistics about students and mobile devices). The lecturers also use tablets to interact with delivered content. During the analysis of the use case, we confirmed some well-known observations. We split the observations by whether they concern the presenter or the audience.

From the perspective of a lecturer, there is only a limited amount of time to present a predefined set of information. A big audience with more than 30 people makes it difficult to interact with every listener on a personal level. Many speakers enrich their talks with slides as an additional visual channel. Some information require prior knowledge. To ensure a high level of comprehension, lecturers structure the presented information to meet prior requirements. Information is explained within time constraints and as extensive as subjectively needed. It is well-known that people explain things the way they understand them. A lecturer dedicated to a certain topic structures information influenced by his comprehensive contextual knowledge.

A receiving audience is a set of heterogeneous persons. It is well-known that humans differ in level of interests, distractibility, preliminary knowledge, environmental context and perception capacity. While comprehension can be seen as correlated to contextual knowledge, interest is correlated to the level of comprehension. As described in [Tob94], there is a linear relation between contextual knowledge and interest. The level of attention may also be connected to the level of interest. Missing prior information either through missing attention or comprehension may lead to a lack of attention and missing comprehension of following information. Subsequently, it may be hard for a listener to understand all findings based on this missing information.

The connection of both perspectives shows that it is very difficult to structure information to match the heterogeneous requirements of a big audience. A missing comprehension of individuals leads to an absence of understanding and less attention to subsequent information. While some approaches use mobile devices as direct interface to the presenter [VSL+14, Top14], we focus on supporting individual needs through interaction with presented content.

From an application's view, our approach is to use mobile devices as an ad hoc extension to existing presentation environments. Mobile devices can be used as additional individual visualization channels. Additionally, mobile devices can be used as an interface to interact with delivered content. We try to identify a set of interactions to attribute these delivered information entities based on individual requirements. These ratings may include levels of comprehension and interests. By collecting and processing these ratings, we want to support each user by providing auxiliary information before and during a presentation. To post process delivered content, we suggest repetition mechanisms adapted to requirements of an individual student. We also plan to support the lecturer by reporting the consensual comprehension level and the audience's interactions.

To achieve this goal from a technical perspective, we reviewed multi-display environments. We identified technical issues as well as adapted requirements in mobile multi-display

environments such as visibility and dynamic display spaces. We then analyzed recent software developments regarding mobile devices. For our requirement we choose hybrid architectures which enable a persistent sharing of web based content and functionality between different operating systems on run time [Bud].

On conceptual level, we define a set of interactions that can be performed on a mobile device to handle and classify information during a lecture. By now, the classification includes ”interesting”, ”missing comprehension”, and ”already known”. These actions will be used to adapt our information model.

Our first approach to build an information model is based on a graph containing information entity nodes and a set of different relation edges. While information entity nodes can contain any content or information being delivered in a lecture, relation edges shall define different levels of semantic and temporal proximities.

In contrast to a straight forward slide show, we use this information model to relate content on diverse levels. Some information is required to understand other pieces of information, some is by default not shown in the presentation. Auxiliary information such as interesting facts, examples, and explanations from a differing viewing angle can be requested on demand. While some proximities can be defined by the presenter in advance, others may be spontaneously influenced or generated as response to audience interactions.

Feedback such as interest, level of comprehension, and group consensus which are generated through interactions on delivered content allows inferring the users' state. Interactions performed by the presenter allow insights to spontaneous demands during a talk. The use of this model enables us to structure content and attribute its relations in a flexible way.

After working on this model, we plan to provide an adaptive display mapping. This mapping will include environmental as well as mobile display spaces. Interactions by the audience denoting individual and consensual requirements will spontaneously influence appropriate visual presentation channels to provide auxiliary or accented content. Our idea is illustrated by the following example: An observed missing comprehension leads to an increased importance of prior information. The compensation will result in an adaption of the current presentation by content mapping and distribution over appropriate channels and adaption of learning assistance after a presentation.

3 Conclusions

Our content based approach enables us to support students on a personal level. Following this goal, we observe interactions with content to collect insights to the mental structure and knowledge of single persons and groups. Based on private mobile devices, our approach supports information delivery before, during and after a presentation. That way students attending a lecture can be prepared by preliminary information and repeat presented content afterward. Presenters will be supported through consensual feedback provided by the system. The feedback includes missing contextual information or areas of interests. This may lead to an improvement of a presentation itself over time. Additional learning theory approaches will be included in our information model.

Acknowledgment

This work is supported by the German Research Foundation (DFG) as part of the graduate school MuSAMA (grant no. GRK 1424/1).

References

[Bud] Raluca Budiu. Evidence-Based User Experience Research, Training, and Consulting: http://perma.cc/A7TZ-893F.

[Fit13] Fittkau und Maaß Consulting. w3b.org - Jeder fünfte Fernseher ist nur Second Screen: http://perma.cc/QXQ3-H2AS, 2013.

[Han13] Michael Hanley. Ball State College Student Cell Phone Study Summary February 2013: College Student Smartphone Usage Hits 74%; Tablet Ownership at 30%, 2013.

[Kir14] Thomas Kirste. MuSAMA - Multimodal Smart Appliance Ensembles for Mobile Applications: http://perma.cc/SKD5-3RED, 2014.

[KXAA13] W. Z. Khan, Yang Xiang, Mohammed Y. Aalsalem, and Quratulain Arshad. Mobile Phone Sensing Systems: A Survey. *Communications Surveys Tutorials, IEEE*, 15(1):402–427, 2013.

[Pri14a] Primate Labs Inc. Geekbench Browser Android Benchmarks: http://perma.cc/4G3V-56VT, 2014.

[Pri14b] Primate Labs Inc. Geekbench Browser Benchmark iPhone, iPad, and iPod Benchmarks: http://perma.cc/Y4F-YF2S, 2014.

[RLS11] Axel Radloff, Martin Luboschik, and Heidrun Schumann. Smart Views in Smart Environments. In *Smart Graphics*, pages 1–12, 2011.

[RLSS12] Axel Radloff, Anke Lehmann, Oliver Staadt, and Heidrun Schumann. Smart Interaction Management: An Interaction Approach for Smart Meeting Rooms. In *Proceedings of the 8th International Conference on Intelligent Environments (IE'12)*, pages 228–235, Guanajuato and Mexico, 2012. IEEE Computer Society.

[SBSM13] Teddy Seyed, Chris Burns, Mario Costa Sousa, and Frank Maurer. From Small Screens to Big Displays: Understanding Interaction in Multi-display Environments. In *Proceedings of the Companion Publication of the 2013 International Conference on Intelligent User Interfaces Companion*, IUI '13 Companion, pages 33–36, New York and NY and USA, 2013. ACM.

[Sey13] Alemayehu Seyed. *Examining User Experience in Multi-Display Environments*. PhD thesis, University of Calgary, Calgary, 2013.

[Tob94] Sigmund Tobias. Interest, Prior Knowledge, and Learning. *Review of Educational Research*, 64(1):37–54, 1994.

[Top14] Top Hat Monocle Inc. TOPHAT - Make every lecture count: http://perma.cc/NHJ4-6NL5, 2014.

[VSL+14] Jonas Vetterick, Bastian Schwennigcke, Andreas Langfeld, Clemens. H. Cap, and Wolfgang Sucharowski. Making Classroom Response Systems More Social, 2014.

[ZL04] Frank Zhao and Qiong Liu. A Web Based Multi-display Presentation System. In *Proceedings of the 12th Annual ACM International Conference on Multimedia*, MULTIMEDIA '04, pages 176–177, New York and NY and USA, 2004. ACM.

Optimizing session-based HTTP flood detection

Dmytro Piatkivskyi, Slobodan Petrovic
Gjøvik University College
email: dmytro.piatkivskyi@gmail.com, slobodan.petrovic@hig.no

Abstract: HTTP flood attacks keep being among the most prevalent attacks for the decades and the damage caused by these attacks is growing every year. An HTTP flood sends massive, but legitimate HTTP traffic to a victim from multiple sources. This highly degrades the performance of the target server and it will eventually stop functioning at some point having all the resources exhausted. The task of mitigating the effect of an HTTP flood is very challenging by itself, yet there are many factors that make it even more complicated. One of such complications is that HTTP is a sessionless protocol. In order to design a session-based HTTP flood detection system, an HTTP session needs to be defined. The chosen definition affects the performance of the end system to a large extent. In this paper, we study what session definition is appropriate for online HTTP flood detection. After that, an experiment is run to define the values of the session parameters that facilitate the best detection performance of HTTP flood mitigation systems.

1 Introduction

An HTTP flood is a type of Distributed Denial of Service attack, which runs on the application layer of the OSI model. Such attacks are conducted by simply sending many legitimate looking requests to a web server, exhausting all its resources. Having all the resources exhausted, a web server stops serving legitimate requests at some point violating the availability property. This causes inevitable loss of money and reputation, and drives the users away. The task for a defender is to make sure that legitimate users still get the requested pages within a reasonable period of time.

The paper describes an attempt to improve the efficiency of HTTP flood detection (mitigation) systems [1]. The main focus is to detect as many different sophisticated attacks as possible taking into consideration flash events. An enhanced mitigation system would never completely eliminate the threat, but it may render many known attacks inefficient. In this way, an attacker would be forced to spend more resources and money to reach his or her goals making it eventually unattractive activity.

The paper is organized as follows. It starts with an overview of HTTP flood mitigation solutions. Then, having defined an HTTP session in Section 3, the influence of session parameters choice is studied in Section 4. Finally, conclusions are given in Section 5.

[1] Hereafter we use terms ”detection” and ”mitigation” interchangeably

2 Mitigation techniques

2.1 Machine learning techniques

First papers that described using machine learning for traffic segregation were written on search robots detection [PPLC06] [TK02]. Tan et al. [TK02] used C4.5 decision tree algorithm to classify and hence distinguish robot and human browsing activity.

One of the first approaches to HTTP flood mitigation was by modeling user browsing behavior, mostly with Hidden semi-Markov Model (HsMM) to describe the browsing behavior of users [YSz] [JXKb] [YSz09]. The technique is based on document popularity and transmission probabilities between pages. It is effective as far as an attacker does not mimic user behavior, which is quite possible. It also suffers from high computational complexity, which makes it unsuitable for online detection. The idea of using transmission probabilities between pages to detect bots was further studied in [CKC] [OM]. The main reasoning behind is that a bot is not aware of probability with which a link on a page is clicked on.

Intuitively, clustering seems to be a proper family of algorithms for attack and normal traffic segregation [CKC] [JZHX]. The clustering can first be done on normal traffic to see normal usage patterns. After this, any deviations from defined clusters are treated as attack sessions. Jie et al. [JZHX] introduced a way to interpret such deviations. They defined a trust value which takes into account the proximity to the nearest cluster and importance of that cluster. Paper [CKC] describes hierarchical clustering applied to the problem. Having defined four features to work with, the authors achieved acceptable results. The detection rate reaches 90% which is good enough for the purpose of HTTP flood mitigation, although the false positive rate, which is more important, is not given.

In [RSS] Support Vector Machine (SVM) was used to classify traffic and detect attacks. Oikonomou et al. [OM] reached very low False Positive rates with decision trees.

2.2 Other approaches

Since the goal of HTTP floods is to send as many requests as possible while remaining undetected, it is reasonable to limit the rates at which the connections are accepted [RSU$^+$09] [HIKC]. In [RSU$^+$09], Ranjan et al. presented a scheme where a suspicion measure is assigned to each session according to session inter-arrival times, request inter-arrival times, and session workload profile. Further, the requests are scheduled according to its session suspicion measures. If a server queue is full, requests from the most suspicious sessions are dropped.

Another way to characterize user access behavior is through web-page clicking ratio [JXKb] [JXKa] which expresses page popularity. The approach assumes that all users access the same (so called ”hot”) pages. ConnectionScore scheme [BD12] measures various statistical properties of users and the traffic they generate and compare these properties to the

model. If there are significant deviations, the users are blocked.

Paper [SIYL06] does not even attempt to distinguish a DOS attack request from the legitimate ones. Instead, it schedules an incoming request according to the workload of the session it belongs to. This way, the aggressive users will be penalized and good clients will get more resources. Papers [OM] [GCD] suggest using deception techniques. The idea is to embed invisible objects with hyperlinks into a page and mark those users who requested such links as bots.

The very promising and effective approach against application layer floods is CAPTCHA puzzles [KKJB05] [MSC+03]. These are challenge-response tests that tell humans and computers apart.

Works [JZHX] [WVB+06] [NPDD12] implement currency method where a request is served only after a client pays for it. For example, in [JZHX] when a server is overloaded it drops the session connections and asks to retry immediately. Paper [NPDD12] describes a scheme where the client's machine is supposed to solve a puzzle sent by the requested server. To solve a puzzle of defined complexity, a client must pay with CPU time.

3 An HTTP session definition

3.1 Attempts to define an HTTP session

HTTP is a sessionless protocol [New00]. Nevertheless, the notion of an HTTP session is used quite often. Divergence in the definition of an HTTP session in many papers inspired scientists to study what actually an HTTP session is [MDG+09]. Often, notion of a session is defined prior to conducting the actual work pertaining HTTP such as workload characterization [MAFM99], traffic analysis [QLC05] [Coo00], user behavior characterization, etc. Most approaches to HTTP flood mitigation also require HTTP session to be defined [RSU+09] [CC04]. In this section, we first discuss the definitions of other authors and then give our own on which the later reasonings are based.

It is trivial to define session so that a human understands it. According to [MAFM99], a session is a sequence of requests of different types made by a single client during a single visit to a web site. This definition is clear and brings no confusion. But the problem is that in technical sense it is almost impossible to determine a session. It is so due to many factors such as the fact that some users may share the same IP address and not all user requests are sent to the server (some responses might be cached in a user's web-browser), etc. In [CC04], the logical access sequences and the physical access sequences are differentiated. According to this paper, the physical access sequences are those that are actually requested and therefore logged in the access log of a web server. At the same time, the logical access sequences are those that correspond to the user's actions and what the user actually clicks on. Further, paper [CC04] states that it is infeasible to detect anomalous sessions based on logical access sequences due to the fact that it is impossible to track user's clicks. Hence, researchers focused on retrieving a session from mainly web server's logs or incoming traffic analysis.

According to [Coo00], a session can be identified by the referrer field taking into account that referrer of current request of a session must match one of the URLs previously requested in this session. Paper [QLC05] introduced the concept of referrer tree, which was used to aggregate requests into sessions using the timeout as well. An improved algorithm for constructing the referrer tree was described in [MDG+09], which was agnostic to timeouts. This algorithm segments a click stream into logical sessions based on referrer information. Every segment corresponds to a session.

A quite opposite approach was used in [RSU+09] where authors took HTTP/1.1 persistent connections as a base for session-oriented connections. This approach does not reflect the human understandable definition of a session since it lasts as long as the TCP socket is kept opened. For example, for the Apache 2.2 web server the default connection timeout is 5 seconds. That means that if a user spends more than 5 seconds on reading a page and then clicks on a link, a new session will be initiated. One must understand that persistent sessions were introduced for optimal resource usage, not to define an HTTP session. The interesting fact though is that in this case inter-session arrival time can be close to zero (e.g. 0.2 seconds) which introduces the concept of session flooding.

3.2 The proposed definition

Most HTTP flood mitigation systems, [JXKb] [CKC] to name a few, are session-based. But HTTP is a sessionless protocol [New00], which means that we need to define what a session is in order to implement a session-based flood detection. Most papers use an HTTP session definition based solely on a timeout.

Values for the timeout vary to a large extent from a minute [MDG+09] to 30 minutes [JXKb] [CKC] [CP95]. Paper [MDG+09] states that the timeout is chosen arbitrarily and there is no justification for any specific value. Besides, the choice of the timeout changes all the relevant statistic. In spite of this, we have decided to use the session definition by a timeout. Moreover, in our experiment we seek for the proper value of the timeout for HTTP flood detection, i.e. such timeout that makes the best statistic of a session for detection.

A very important requirement for an HTTP flood detection system is to handle traffic efficiently in real time. Obviously, it is a bad idea to use the given HTTP session definition in real time systems. There are many questions to answer. Should we wait until a session is complete (N seconds since the last request received), in order to decide on this session? Or should we calculate a session's statistic having received a sufficient number of requests? What should the number be? If we would have defined the proper sufficient number, there is an open question left whether requests in a session get obsolete. A session defined simply by a timeout can last for a very long time. Does it mean that requests received hours (or minutes) ago become obsolete and should not be counted into the session statistic? We tried to answer all these questions at once, introducing another parameter to the session definition, which is the "last M requests". This parameter is introduced specifically for online detection. A session statistic may change with time. Having a very long session

with many requests, a new request would not change statistic much even if the request is an outlier. The statistic of recent requests is more important in a real time detection system. Moreover, counting only last M requests decreases usage of CPU and memory resources.

Another implementation trick pertaining the M parameter is that sessions that consist of less than M requests are not considered at all. Indeed, HTTP flood bots send massive traffic to a target. And if there is not enough requests in a session to make robust statistic, then such a session is not an attack session.

Thus, we give the following HTTP session definition:

> An HTTP session is a sequence of last M HTTP requests received from one user while the time difference between two consecutive requests is less than a timeout N.

In this way, we defined an HTTP session by two parameters, namely timeout N and last M requests. These two parameters are further investigated in the next section.

4 Session parameters choice

We now study how the choice of the timeout N and the number of last M requests affect the detection accuracy of HTTP flood mitigation systems. For that we generate a dataset and group the requests from the dataset into sessions following the proposed definition of an HTTP session. Then we implement the selected features and calculate those features for each session. The set of features makes a session statistic. At this step, we have a list of session features along with a class label. Then we run machine learning algorithms on the list of session features and we analyze the performance of the algorithms.

4.1 The dataset

The dataset we have generated for the experiment consists of attack and background traffic. As background traffic, we have chosen the publicly available 1998 Football World Cup dataset, which represents a flash event occurred during FIFA World cup in 1998. Based on the background traffic, attack traffic has been generated that consists of many different types of HTTP flood.

Attack traffic represents many different HTTP flood attacks. To generate it, we proposed a model of HTTP flood. The attack is modeled by three parameters: request rate, ON/OFF periods and page distribution. Thus, an attack can be described by a three-tuple

$$\mathcal{A} = \{\mathcal{R}, \mathcal{ON\_OFF}, \mathcal{D}\}, \text{ where}$$

$\mathcal{R} = \{r | r \text{ is a request rate}\}$,
$\mathcal{ON\_OFF} = \{< on, off > | on \text{ is a period of time of being active,}$

off is a period of time of being inactive $\}$,
$\mathcal{D} = \{d | d$ is distribution of requested pages$\}$.
The following values of attack model parameters were chosen:

$\mathcal{R} = \{0.05, 0.1, 0.5, 1.0, 5.0\}$,
$\mathcal{ON\_OFF} = \{< 1, 9 >, < 5, 5 >, < 9, 1 >, < 10, 90 >, < 50, 50 >, < 90, 10 >\}$,
$\mathcal{D} = \{$uniform distribution, distribution by popularity, distribution by size$\}$.

4.2 Selected features

The following five features were selected:

1. Request rate
2. Popularity of accessed objects
3. Uptime to downtime proportion
4. Diversity of accessed pages
5. Average size of objects

4.3 Analysis of an HTTP session definition

We conduct the experiment in two steps. First, we fix parameter M and run the simulated system with different values of parameter N. We range N parameter from 30 to 1000 seconds. We believe that lower value than 30 seconds of N would segment flow of requests into very small sessions. Such small (in terms of number of requests it consists of) sessions would have weak and not stable statistic. On the contrary, a higher value than 1000 seconds does not bring great difference into session statistic, but extends the period of time during which we keep the session alive. In a real time system, a session queue needs to be maintained until the timeout is reached since the last request was received. That means, the longer the session timeout is, the longer it needs to be in memory. Hence, it is very inefficient to have very long timeouts.

J48, MultilayerPerceptron and ThresholdSelector algorithms were chosen for the experiment.

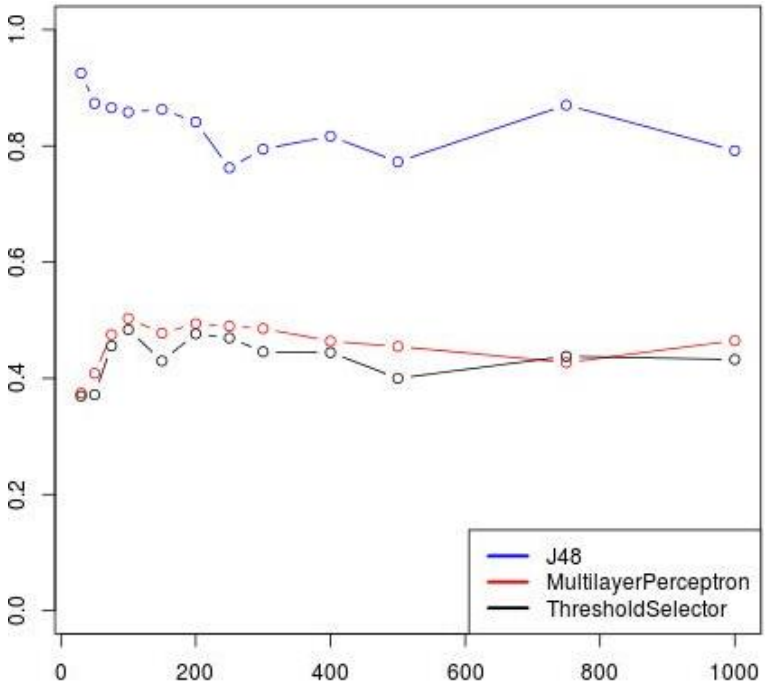


Figure 1: Dependency of detection accuracy on N parameter

We do not consider True Negatives (TN) and False Positives (FP) in our experiment, because all the legitimate sessions have to be detected as legitimate due to our policy. It means that FP are not accepted at all and TN has to be as close to 1 as possible. Although it is usually not possible to achieve TN = 1, in all our experiments it is equal to 0.99 or higher.

Figure 1 shows that detection accuracy does not change much with the N parameter. We see a better performance of J48 algorithms with small values of N (less than 50). But at the same time, Multilayer Perceptron and Threshold Selector perform badly with small values of N. Moreover, we believe that J48 performs well with small values of N because of overfitting. Since starting from $N = 200$ there are only minor deviations and the detection accuracy is about the same, we conclude that the most common choice of $N = 300$ is appropriate for HTTP flood detection as well. In all further experiments we use $N = 300$.

The second step of the experiment is analysis of the parameter M of the session definition. For that, we fix parameter N equal to 300 and run the system simulation with different values of the parameter M. We range the parameter M in the same way as the parameter N - from 30 to 1000 requests. The reasoning behind is that less than 30 requests in a session results in a weak and unstable session statistic. Moreover, even if a server serves 30 attack, requests that will not harm much. Besides, in flooding attacks, there will be definitely more than 30 requests. On the other hand, too high value of M parameter means late detection, since we need to collect M requests before we calculate a session statistic.

It also increases the cost of maintaining a session queue and re-calculating the statistic. We have chosen the same values for M as for N. The algorithms are the same as well.

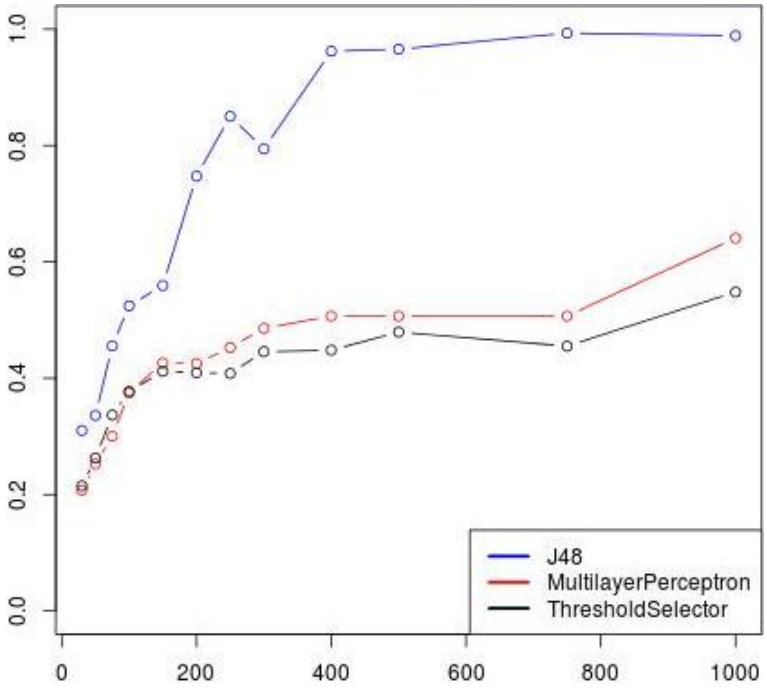


Figure 2: Dependency of detection accuracy on M parameter

From the Figure 2 we see that detection accuracy increases with M up the to point $M = 400$. Further, the detection accuracy does not change much. There is also a slight performance improvement at the point $M = 1000$ for Multilayer Perceptron and Threshold Selector algorithms. The manual investigation shows that it is due to introducing False Positives, which are very undesirable. To take a closer look, ROC curves were built (see Figure 3). Surprisingly, the algorithm has worse performance for $M = 1000$ than for $M = 400$. This confirms that high values of the parameter M might even decrease the detection accuracy of an HTTP flood detection system. This confirms our choice of the proper value of M, which is 400 requests.

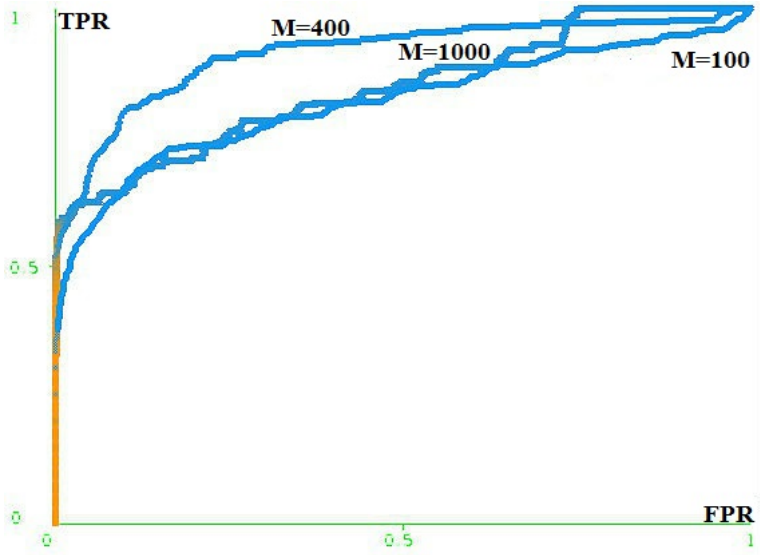


Figure 3: ROC curves for the Multilayer Perceptron algorithm

4.4 Analysis of detection rate by attack type

In order to analyze detection accuracy by attack type, the detection performances of Multilayer Perceptron algorithm for $M = 300$ and $M = 750$ have been examined. Simple comparison of detection accuracies revealed some tendencies. Thus, having normal request rate only volumetric attacks (attacks distributed by size) can be detected. This means that volumetric attacks are the easiest to detect. At the same time, attacks that guess popularity of pages are the most difficult to detect. In addition, it has been concluded that the ON/OFF parameter of the proposed attack model does not influence the detection accuracy. It also means it does not influence an attacker's ability to stay stealth, which means that there is no need to model it.

In order to investigate how detection accuracy changes with the parameter M for each attack type, we compare performances of the Multilayer Perceptron algorithm with $M = 300$ and $M = 750$.

Interestingly enough, attacks that simulate uniform distribution are worse detected using a higher value of the parameter M (see Tables 1 and 2). But, what is more noteworthy is that attacks that simulate popularity distribution are better detected with $M = 750$ (see Tables 3 and 4). We believe that these two types of HTTP flood are detected, in general, due to three features, namely *request rate*, *average popularity of objects* and *diversity of objects*. They are not detected by *average size of object* feature, because their average size of objects in a session is equal to those of legitimate sessions. Further, as it was concluded in this section earlier, ON/OFF periods do not influence detection much. And,

consequently, *uptime/downtime proportion* (*ON/OFF proportion*) feature does not detect any attack.

Attack type	Not detected sessions	Detected sessions
uniform_0.5_1_9	1341	293
uniform_1_1_9	406	2895
uniform_0.5_5_5	1182	299
uniform_1_5_5	922	2406

Table 1: Detection performance of Multilayer Perceptron for $M = 300$

Attack type	Not detected sessions	Detected sessions
uniform_0.5_1_9	1184	0
uniform_1_1_9	2851	0
uniform_0.5_5_5	1031	0
uniform_1_5_5	2878	0

Table 2: Detection performance of Multilayer Perceptron for $M = 750$

Comparing the results of attacks of the same rate, we exclude influence of *request rate* feature, which leaves us only two features. In this way we conclude that difference in detection we observe in this experiment is due to performance of *average popularity of objects* and *diversity of objects* features. In other words, the value of the M parameter that is equal to 300 facilitates the features *average popularity of objects* and *diversity of objects* to detect attacks that simulate uniform distribution. On the other hand, the value of the M parameter that is equal to 750 facilitates the features *average popularity of objects* and *diversity of objects* to detect attacks that simulate popularity distribution.

Attack type	Not detected sessions	Detected sessions
bypopularity_1_1_9	3324	0
bypopularity_5_1_9	533	17168
bypopularity_1_10_90	3313	0
bypopularity_5_10_90	49	17619

Table 3: Detection performance of Multilayer Perceptron for $M = 300$

All the discussion above leads to two most important conclusions:

1. Each feature reaches its best utility with different values of parameter M. It means that the proper value of the parameter M should be defined for each feature independently.

Attack type	Not detected session points	Detected sessions
bypopularity_1_1_9	2378	496
bypopularity_5_1_9	275	16976
bypopularity_1_10_90	2286	577
bypopularity_5_10_90	105	17113

Table 4: Detection performance of Multilayer Perceptron for $M = 750$

2. Two different values of the parameter M facilitate detection of different attacks with the same feature. It suggests using multiple instances of the same feature calculated for different values of parameter M.

5 Conclusions

This research was set out to explore the field of HTTP flood mitigation and to optimize session-based HTTP flood detection. The goal was not to develop a new detection system that performs better than the others, but rather to enhance existing systems and guide designers while developing new ones.

An HTTP session has been defined by two parameters, which were further investigated in the experimental study, namely timeout N and number of last M requests. The experimental analysis showed that the choice of the timeout N does not influence the detection accuracy of HTTP flood attacks as far as it is high enough (more than 200 seconds). That confirmed the common practice found in the literature of using timeout of 300 seconds. Oppositely, it has been shown that the number of last requests M does influence the detection rate. It has also been experimentally determined that the best performance is reached with $M = 400$ requests.

It has been identified that different features reach their maximum utility with different values of M. Moreover, different values of the parameter M facilitate detection of different types of HTTP flood, even by the same feature. This results in a necessity to conduct further analysis for each feature and each type of HTTP flood.

References

[BD12] Hakem Beitollahi and Geert Deconinck. Tackling Application-layer DDoS Attacks. *Procedia Computer Science*, 10(0):432–441, 2012.

[CC04] Sanghyun Cho and Sungdeok Cha. SAD: web session anomaly detection based on parameter estimation. *Computers & Security*, 23(4):312 – 319, 2004.

[CKC] Ye Chengxu, Zheng Kesong, and She Chuyu. Application layer ddos detection using clustering analysis. In *Computer Science and Network Technology (ICCSNT), 2012*

2nd International Conference on, pages 1038–1041. no false positive rate stated.

[Coo00] Robert Walker Cooley. Web Usage Mining: Discovery and Application of Interestin Patterns from Web Data, 2000.

[CP95] Lara D. Catledge and James E. Pitkow. Characterizing browsing strategies in the World-Wide web. *Computer Networks and {ISDN} Systems*, 27(6):1065 – 1073, 1995. Proceedings of the Third International World-Wide Web Conference.

[GCD] D. Gavrilis, I. Chatzis, and E. Dermatas. Flash Crowd Detection Using Decoy Hyperlinks. In *Networking, Sensing and Control, 2007 IEEE International Conference on*, pages 466–470.

[HIKC] Liu Huey-Ing and Chang Kuo-Chao. Defending systems Against Tilt DDoS attacks. In *Telecommunication Systems, Services, and Applications (TSSA), 2011 6th International Conference on*, pages 22–27.

[JXKa] Wang Jin, Yang Xiaolong, and Long Keping. A new relative entropy based app-DDoS detection method. In *Computers and Communications (ISCC), 2010 IEEE Symposium on*, pages 966–968.

[JXKb] Wang Jin, Yang Xiaolong, and Long Keping. Web DDoS Detection Schemes Based on Measuring User's Access Behavior with Large Deviation. In *Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE*, pages 1–5.

[JZHX] Yu Jie, Li Zhoujun, Chen Huowang, and Chen Xiaoming. A Detection and Offense Mechanism to Defend Against Application Layer DDoS Attacks. In *Networking and Services, 2007. ICNS. Third International Conference on*, pages 54–54.

[KKJB05] Srikanth Kandula, Dina Katabi, Matthias Jacob, and Arthur Berger. Botz-4-sale: surviving organized DDoS attacks that mimic flash crowds, 2005.

[MAFM99] Daniel A. Menascé, Virgilio A. F. Almeida, Rodrigo Fonseca, and Marco A. Mendes. A Methodology for Workload Characterization of E-commerce Sites. In *Proceedings of the 1st ACM Conference on Electronic Commerce*, EC '99, pages 119–128, New York, NY, USA, 1999. ACM.

[MDG+09] Mark Meiss, John Duncan, Bruno Gon, J. Ramasco, and Filippo Menczer. What's in a session: tracking individual behavior on the web, 2009.

[MSC+03] William G. Morein, Angelos Stavrou, Debra L. Cook, Angelos D. Keromytis, Vishal Misra, and Dan Rubenstein. Using graphic turing tests to counter automated DDoS attacks against web servers, 2003.

[New00] Jan Newmarch. HTTP Session Management, August 2000.

[NPDD12] Raju Neyyan, Ancy Paul, Mayank Deshwal, and Amit Deshmukh. Article: Game Theory based Defense Mechanism against Flooding Attack using Puzzle. *IJCA Proceedings on Emerging Trends in Computer Science and Information Technology (ETCSIT2012) etcsit1001*, ETCSIT(5):6–10, April 2012. Published by Foundation of Computer Science, New York, USA.

[OM] G. Oikonomou and J. Mirkovic. Modeling Human Behavior for Defense Against Flash-Crowd Attacks. In *Communications, 2009. ICC '09. IEEE International Conference on*, pages 1–6.

[PPLC06] KyoungSoo Park, Vivek S. Pai, Kang-Won Lee, and Seraphin Calo. Securing web service by automatic robot detection, 2006.

[QLC05] Feng Qiu, Zhenyu Liu, and Junghoo Cho. Analysis of user web traffic with a focus on search activities. *In Proc. International Workshop on the Web and Databases*, pages 103–108, 2005.

[RSS] A. Ramamoorthi, T. Subbulakshmi, and S. M. Shalinie. Real time detection and classification of DDoS attacks using enhanced SVM with string kernels. In *Recent Trends in Information Technology (ICRTIT), 2011 International Conference on*, pages 91–96.

[RSU+09] S. Ranjan, R. Swaminathan, M. Uysal, A. Nucci, and E. Knightly. DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks. *Networking, IEEE/ACM Transactions on*, 17(1):26–39, 2009. asymmetric attack is low rate attack, the detection is based on statistical properties of normal user profiles.

[SIYL06] Mudhakar Srivatsa, Arun Iyengar, Jian Yin, and Ling Liu. *A Middleware System for Protecting Against Application Level Denial of Service Attacks*, volume 4290 of *Lecture Notes in Computer Science*, chapter 14, pages 260–280. Springer Berlin Heidelberg, 2006. good threat model, many references in related work, could be worth looking at them.

[TK02] Pang-Ning Tan and Vipin Kumar. Discovery of Web Robot Sessions Based on their Navigational Patterns. *Data Mining and Knowledge Discovery*, 6(1):9–35, 2002.

[WVB+06] Michael Walfish, Mythili Vutukuru, Hari Balakrishnan, David Karger, and Scott Shenker. DDoS Defense by Offense. In *ACM SIGCOMM 2006*, Pisa, Italy, September 2006.

[YSz] Xie Yi and Yu Shun-zheng. A Novel Model for Detecting Application Layer DDoS Attacks. In *Computer and Computational Sciences, 2006. IMSCCS '06. First International Multi-Symposiums on*, volume 2, pages 56–63.

[YSz09] Xie Yi and Yu Shun-zheng. Monitoring the Application-Layer DDoS Attacks for Popular Websites. *Networking, IEEE/ACM Transactions on*, 17(1):15–25, 2009.

Exploring Classroom Response Systems in Practical Scenarios

Benjamin Leiding, Jonas Vetterick and Clemens H. Cap

Department of Computer Science
University of Rostock
Albert-Einstein-Str. 22
18059 Rostock, Germany
email: {benjamin.leiding,jonas.vetterick,clemens.cap}@uni-rostock.de

Abstract: The increasing number of students per classroom requires new ways of interactions betweens teachers and students. Classroom Response Systems (CRS) aim to solve this problem by enabling feedback for large audiences. We defined and identified requirements of a viable solution and present Tweedback as a example of modern Classroom Response Systems. Tweedback is a web application and provides different types of feedback: A chatwall, where the audience can ask questions, a panic-button to provide immediate feedback on the lecturers presentation and multiple choice questions. Tweedback has activeley been used since January 2013. The feedback of our users and our own practical experiences allowed us to identify several issues of Classroom Response Systems and develop suitable solutions.

1 Introduction

The number of students at german universities has increased substantially in the last two decades, from 1.7 million in 1990 to 2.6 million in 2013 [SB14]. As a result the number of students per classroom increased the same way. For some courses a single lecture hall isn't enough anymore so lectures are streamed to different classrooms simultaneously. These circumstances call for an adapted method of interaction between students and teachers. In small classrooms students can interact directly with their lecturer, but with large audiences direct communication is limited to only a few students. There are several reasons for this. The large number of students makes it impossible to get feedback from each of them in a reasonable time. Another reason is that students might be afraid to ask or answer questions in front of large audiences, because they feel uncomfortable or don't want to give a wrong answer.
One strategy to re-establish a viable feedback channel in classrooms of this size are Classroom Response Systems (CRS). Classroom Response Systems provide different types of feedback [GVC13] and can be used with large audiences. Some of them provide only one form of feedback, for example multiple choice questions [KL09]. Others combine different forms of feedback. The authors developed a Classroom Response System called Tweedback. Tweedback is implemented as a web application and provides three forms of

feedback. Firstly, a chatwall where students can post questions. Secondly, different kinds of multiple choice surveys. The third one, a Panic-button to provide immediate feedback on the lecturers presentation. We rolled out the first version of Tweedback in January 2013 . Since then we received a lot of feedback from our users which helped us to identify general problems of Classroom Response Systems in general and missing features of Tweedback. In this paper we will focus on practical scenarios, experiences and issues of our system.
This publication is organized as follows. In the second chapter we will define the requirements of a Classroom Response System that is able to solve the described problem. Chapter three gives an overview of the state of the art of Classroom Response Systems and the forms of feedback they provide. Section four introduces Tweedback and its functions in detail. Section five focuses on practical experiences, user feedback and issues of Classroom Response Systems. The last section summarizes our work so far and outlines our future work.

2 Requirements

At first, a feasible solution has to be easy to set up, even for a non-technical person. A complicated and time consuming setup discourages users to participate in Tweedback. Especially teachers with no technical background might have problems to handle the system under time pressure. Solutions that use an extra device, as a remote control, are very time consuming to set up. The devices have to be maintained and distributed before and collected after every lecture. Another disadvantage of using hardware devices is bad scalability because there has to be a device for every student. Hardware device-based solutions only scale with the number of remote controls.
Tweedback is a feedback system for large audiences hence scalability is an important criteria. Unlike traditional feedback systems which rely on special external devices to interact with each other Tweedback uses devices that students already have. Administrators only need to take care of our backend so that it can handle the appropriate amount of browsers. According to Bitkom [Bit14], 78% of young german pepople own an internet-capable smartphone, hence Tweedback is implemented as a web application. That lowered the administrative effort and financial cost of our solution and made it much easier to maintain. The downside of this decision is that a permanent internet connection is required. Closely linked to an easy set up is an interface which is fast, intuitive, user friendly and suitable for mobile devices.
Tweedback is designed to lower the inhibition threshold for our users as much as possible. Therefore we dispensed a user management system and the corresponding initial account creation procedure. This decision results in a further advantage. Without an account it is not possible to link the interactions of Tweedback users to real persons. Anonymity is a very important characteristic of Tweedback. People might be afraid to give a wrong answer or to ask questions in front of large audiences, especially first year students.

3 State of the Art

Traditional Classroom Response Systems (CRS) have been used as voting machines: Teachers asked a multiple choice question and students answered them by clicking on a remote control that provided buttons for each answer [KL09]. As these voting devices are very expensive and have to be maintained, modern CRS use the mobile devices students already have. Since mobile devices, as smartphones, pads or notebooks, provide a display that can draw more than just buttons for multiple choice questions, CRS evolve to comprehensive feedback systems that are able to implement more enhanced functions for feedback [DCC02] [FBSB12] [Jen07] [KSZ+12] [VGC13]. This section provides an overview of current modern Classroom Response Systems and concludes their similarities and differences.
On the one hand there are several academic, free implementations of modern CRS as ARSNova[1], inVote[2], myTU[3], Pingo[4] [KSZ+12], Smile[5] [FBSB12] and Tweedback[6] [VGC13]. All of them, except myTU, have at least the function to ask multiple-choice questions. Furthermore only Pingo does not provide a mechanism to rate teachers' speech parameter, whereas all others do. The possibility for students to ask questions is only provided by myTU, Tweedback and Smile. On the other hand there are non-academic modern CRS, which require a fee to use them. Common representatives are TopHat[7], Ombea[8] and Letsfeedback[9]. All three provide at least a function to ask multiple choice questions [VGDC14].

Regarding the inhibition threshold all of the presented CRS require a registration process for teachers to use the system. Only Tweedback allows anyone to use it's functions without any registration. Moreover all of them are accessible either using a web browser or an app on iOS and/or Android. Concerning the anonymity, all of these modern CRS allow students to provide their feedback anonymously, or at least using a pseudonym [VGDC14].

4 Tweedback

Tweedback is a scalable, web based CRS whichs main purpose is to provide feedback channels between lecturers and their students. Users can access Tweedback through any internetcapable device with a webbrowser. It is designed to be used with large audiences and easy to set up.
The following section we will introduce the three different functions Tweedback provides. All functions can be activated separately in order to minimize distraction through unnec-

[1] https://arsnova.eu
[2] http://invote.de
[3] http://mytu.tu-freiberg.de
[4] https://pingo.upb.de
[5] http://www.smile.informatik.uni-freiburg.de
[6] https://twbk.de
[7] https://tophat.com/
[8] http://www.ombea.com/
[9] http://letsfeedback.com/

essary items on the screen.
The first function is called Chatwall [VGC13]. The participants can post questions to the Chatwall or leave any other kind of text based feedback (Figure 1). Users can read every post on the Chatwall and hide them if they are irrelevant. Especially large audiences can produce several postings per minute which makes it impossible for the lecturer to read them all while giving a presentation. Therefore users can upvote postings which are especially relevant to them. Postings with the most votes are displayed on top of the Chatwall so the lecturer can see the most relevant postings at a glance. This sorting-mechanism minimizes the distraction that the lecturer has to deal with. Teachers are also able to fade out postings, as a result these postings don't appear on the Chatwall anymore. Furthermore it is possible to mark postings, so lecturers can revise all interesting posts after the presentation and find unanswered questions. There might be very helpful questions on the Chatwall with a low vote count because they don't seem to be relevant to the majority of students.
It is also possible to sort the Chatwall to show the newest posting first. This sorting-mechanism is intended to be used by students so they don't miss any new questions. In order to keep the questions short and clear we limited the maximum posting length to 140 characters. We also added a three second timeout between two postings to prevent distracting spam messages.

Figure 1: Chatwall - Student view

The second function provided by Tweedback is the Quiz [GVC13]. Teachers can start different kinds of surveys during the presentation. Tweedback supports simple yes or no questions as well as multiple choice questions with two to five choices. The current answer distribution is visualized in real time (Figure 2) until the lecturer closes the quiz and publishes the results. The audience can only see the published results to avoid an influence of the already given answers on the future answers.

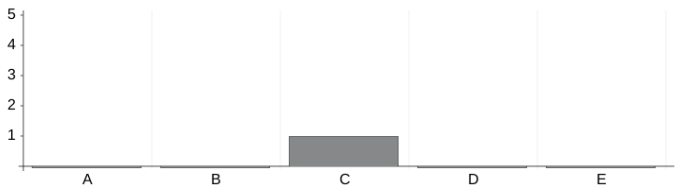


Figure 2: Quiz - Teacher view

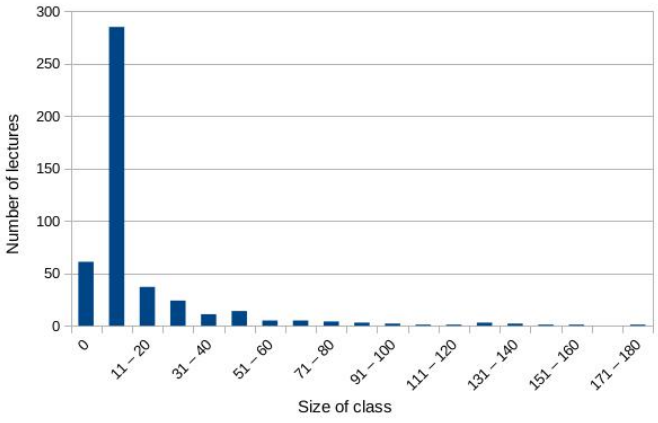
Besides Chatwall and Quiz the audience can provide feedback via the Panic-button. There

are multiple scenarios where a user can press the Panic-button, sometimes also referred to as stop button [GVC13]. The lecturer might be to fast, explained a complex issue in an incomprehensible way or any other situation that makes the user feel uncomfortable. As seen in figure 3, the lecturer gets a graphical interpretation of the current situation in his lecture. The more people press the Panic-button, the bigger the graph grows. The x-axis represents the time and the y-axis the ratio of pressed Panic-buttons to participating users.

Figure 3: Panic Button - Teacher view

5 Observations on Practical Use

We rolled out the first version of Tweedback in January 2013. Since then, Tweedback has been used by 3466 unique users and 16 lecturers of the University of Rostock. There might be other external lecturers among our users but due tue our privacy policy we can't identify them through our logfiles. Figure 4 shows the number of lectures for a specific class size. The real class size might be a bit higher because we counted the logged on devices instead of students present in the classroom. 175 users participated in Tweedbacks biggest lecture so far.



5.1 Exploring Non Technical Problems

Both user groups, lecturers as well as students, provided a lot of helpful feedback. The given feedback helped us to identify unknown problems or missing features of Tweedback. The feedback from lecturers and students also revealed a very different perception of communication in classrooms. Some lecturers argue that most students are not afraid to ask or answer questions in front of the class, whereas almost all students hold the opposite point of view. Especially first year students are afraid to embarrass themselves with wrong answers or ask questions in front of the class.
One particular problem was reported from both, lecturers and students. Teachers tend to focus so much on their presentation that they forget to check the provided feedback channels. They miss new Chatwall posts or feedback via the Panic-button. Especially feedback provided by the Panic-button is closely linked to the current situtation in the classroom and gets less usefull with every passing minute. The lack of response from the lecturer discourages the students from participating. At the moment we are analyzing several strategies to overcome this problem. One approach would be to use an acoustic or optical signal to get the lecturers attention. Another possible approach is a notification by a smartwatch. A smartwatch is similar to a smartphone. It is a small mobile computing device with a touchscreen and is worn on the user's wrist. The smartwatch can communicate with other devices and the user can install applications to expand its functionality. Tweedback's notifications are shown on the smartwatch's display.

Some lecturers also reported another serious issue. Contrary to our expectation the setup and use of Tweedback overwhelmed them. A few struggled to comprehend the full functionality of Tweedback instantly, so they missed important information. For example they stopped multiple choice quizes even though less than 50% of the students had voted for an answer. Other lecturers misinterpreted the function of the Quiz and expected to be able to specify their own custom answers instead of using the standard multiple choice answers (A-B-C-D-E).
This problem occured more frequently with teachers from non-technical faculties. However even lecturers of computer science without any CRS experience struggeled with Tweedback. There is a technical and non-technical approach to this problem. The lecturers can participate in a workshop or briefing (non-technical) or work through an interactive tutorial on their own (technical). Both approaches are intended to make the users familiar with the setup and functions of Tweedback, as well as the best practices on how to use a Classroom Response System in reality [BVC14].
The limitiation of one post every three seconds per student in combination with our voting-mechanism proved to be an effective anti-spam strategy. The character limit per posting forced the users to keep their questions short.
We also received suggestions for new features to implement in future versions of Tweedback. Students from technical disciplines suggested a support of Latex to post formulas on the Chatwall. Others asked for a reply function so users can answer chatwall questions. We will evaluate the pros and cons of these suggestion and implement them if appropriate.

5.2 Technical Problems

We faced different technical problems during the development and testing of Tweedback. Our biggest problem, besides temporary server downtimes, was the insufficient WiFi coverage in some classrooms. The WiFi coverage in most tested classroom is usually very good so there have been no problems at all. Students and lecturers were able to use Tweedback without a hitch. Classrooms which are not covered with WiFi are not usable for Tweedback. As mentioned in an earlier paper of our research group the lectures of medical science are given in rooms of the hospital with its own WiFi for managing patient's data. The patient data have high security requirements therefore only a few areas of the hospital provide an open WiFi access [GVC13]. In cooperation with the local IT administration we installed access points in the hospital to provide a sufficient coverage to use Tweedback. Unfortunately it is not feasible to equip every room with a sufficient number of access points before setting up our system. This strategy is very expensive and time consuming. It also contradicts our goal to offer an easy to set up Classroom Response System.
Tweedback can be packed into a more flexible and more practicle solution, the Tweedbag. The Tweedbag is an all-in-one solution. It consists of a small computing device, for example an Intel NUC, and an access point. The computing device runs a local Tweedback instance and the access point manages all WiFi connections. The lecturer only needs to plug in the power cable and turn on the computing device and access point. We suppose that the Tweedbag solves the problem of insufficient WiFi coverage and also provides a very handy and portable all-in-one solution for conferences and other events.

5.3 The Limits of Tweedback

Every system has its limitations. In case of Tweedback or Classroom Response Systems in general most of them are related to the size of the audience. It does not make sense to use Tweedback in combination with a very small audiene. In that case a direct interaction between all participants demands significantly less effort. Even though Tweedback focuses on large audiences, at one point an audience can be too large for Tweedback. Features like the Panic-button and the Quiz are not limited in number of participants, but the Chatwall loses its use when the lecturer is flooded with incoming messages.
Another limit of Tweedback is closely linked to the lecturers presentation style. Some lecturers prefer to walk around the room most of the time and interact with their audience from face to face. They get their direct, but limited, feedback directly from the audience and a Classroom Response System would interfere with their presentation style.

6 Summary

In order to handle the increasing number of students in classrooms new ways of interactions have to be established. We defined and identified requirements of a viable solution and presented Tweedback as an example of modern Classroom Response Systems. Tweedback provides three forms of feedback to enable interaction between students and the lecturer. Firstly the Chatwall, secondly the Quiz and thirdly the Panic-button. The feedback provided by our users and practical experiences enabled us to improve Tweedback's usability and to identify unknown issues of Classroom Response Systems. In the future we will further investigate strategies to lower the user's inhibition threshold and ways to notify the lecturer about recent Tweedback activites. Furthermore we will continue the Tweedbag's development and perform tests to evaluate the advantages and disadvantes of this approach.

Acknowledgments

This work was supported in part by the German Federal Ministry of Education and Research (BMBF) and the University of Rostock. We gratefully acknowledge the professional and motivating atmosphere offered by them in supporting our study.

References

[Bit14] Bitkom. Smartphones stärker verbreitet als normale Handys, 2014 (Accessed October 3, 2014). http://www.bitkom.org/de/markt_statistik/64046_79598.aspx.

[BVC14] Ulrike Borchardt, Jonas Vetterick, and Clemens H. Cap. Determining the Benefits of Social Media Support in Lecturing. In *Proceedings of the International Conference on Interactive Mobile Communication Technologies and Learning 2014 (IMCL2014)*, 2014. Accepted.

[DCC02] Stephen Draper, Julie Cargill, and Quintin Cutts. Electronically enhanced classroom interaction. *Australian journal of educational technology*, 18(1):13–23, 2002.

[FBSB12] Linus Feiten, Manuel Buehrer, Sebastian Sester, and Bernd Becker. SMILE-Smartphones in Lectures-Initiating a Smartphone-based Audience Response System as a Student Project. In *4th International Conference on Computer Supported Education (CSEDU2012)*, pages 288–293, 2012.

[GVC13] Martin Garbe, Jonas Vetterick, and Clemens H. Cap. Tweedback: Online Feedback System for Large Lectures. In *Informatik 2013, 43. Jahrestagung der Gesellschaft für Informatik e.V. (GI), Informatik angepasst an Mensch, Organisation und Umwelt, 16.-20. September 2013, Koblenz*, pages 270–278, 2013.

[Jen07] Alice Jenkins. Technique and technology: Electronic voting systems in an English literature lecture. *Pedagogy*, 7(3):526–533, 2007.

[KL09] Robin H Kay and Ann LeSage. Examining the benefits and challenges of using audience response systems: A review of the literature. *Computers & Education*, 53(3):819–827, 2009.

[KSZ+12] Dennis Kundisch, Michael Sievers, Andrea Zoyke, Philipp Herrmann, Michael Whittaker, Marc Beutner, Gregor Fels, and Johannes Magenheim. Designing a web-based application to support peer instruction for very large groups. *International Conference on Information Systems 2012*, 2012.

[SB14] Statistisches Bundesamt. Staat & Gesellschaft - Bildung, Forschung, Kultur - Studierende - Statistisches Bundesamt (Destatis) - Anzahl Studierende, 2013 (Accessed October 2, 2014). https://www.destatis.de/DE/ZahlenFakten/Indikatoren/LangeReihen/Bildung/lrbil01.html.

[VGC13] Jonas Vetterick, Martin Garbe, and Clemens H. Cap. Tweedback: A Live Feedback System for Large Audiences. In *5th International Conference on Computer Supported Education (CSEDU2013)*, 2013.

[VGDC14] Jonas Vetterick, Martin Garbe, Andreas Daehn, and Clemens H. Cap. Classroom Response Systems in the Wild: Technical and Non-Technical Observations. *International Journal of Interactive Mobile Technologies*, 8(1):21–25, 2014.

Zero–Forcing Equalisation of Estimated Optical MIMO Channels

André Sandmann, Andreas Ahrens and Steffen Lochmann
Hochschule Wismar, University of Technology, Business and Design
email: a.sandmann@stud.hs-wismar.de, {andreas.ahrens,steffen.lochmann}@hs-wismar.de

Abstract: Within the last years Multiple-Input Multiple-Output (MIMO) transmission has reached a lot of attention in the optical fibre community. Theoretically, the concept of MIMO is well understood. However, practical implementations of optical components are in the focus of interest for further computer simulations. That's why in this contribution the specific impulse responses of the (2×2) MIMO channel, including a 1.4 km multi-mode fibre and optical couplers at both ends, are measured for operating wavelengths of 1326 nm and 1576 nm. Since semiconductor diode lasers, capable of working at different wavelengths, are used for the characterization of the underlying optical MIMO channel, inverse filtering is needed for obtaining the respective impulse responses. However, the process of inverse filtering also known as signal deconvolution is critical in noisy environments. That's why different approaches such as Wiener and parametric filtering are studied with respect to different optimization criteria. Using these obtained impulse responses a baseband MIMO data transmission is modelled. In order to create orthogonal channels enabling a successful transmission, a MIMO zero–forcing (ZF) equaliser is implemented and analysed. Our main results given as an open eye-diagram and calculated bit-error rates show the successful implementation of the MIMO transmission system.

1 Introduction

Aiming at further increasing the fibre capacity in optical transmission systems the concept of MIMO, well studied and wide-spread in radio transmission systems, has led to increased research activities in this area [SSB08, Win12, RFN13]. Theoretical investigations have shown that similar capacity increases are possible compared to wireless systems [KÖ6, TV05]. The basis for this approach is the exploitation of the different optical mode groups.

However, the practical implementation has to cope with many technological obstacles such as mode multiplexing and management. This includes mode combining, mode maintenance and mode splitting. In order to improve existing simulation tools practical measurements are needed. That's why in this contribution a whole optical transmission testbed is characterized by its respective impulse responses obtained by high-bandwidth measurements.

In order to describe the optical MIMO testbed at different operating wavelengths semiconductor laser diodes with a pulse width of 25 ps are used. Since the used picosecond laser generator doesn't guarantee a fully flat frequency spectrum in the region of interest,

inverse filtering has to be applied to obtain the MIMO impulse responses. However, the process of inverse filtering also known as signal deconvolution is critical in noisy environments. That's why different approaches such as Wiener and parametric filtering are studied with respect to different optimization criteria such as the mean square error (MSE) and the imaginary error parameter introduced by Gans [Gan86].

Using the measured impulse responses a MIMO baseband transmission system can be constructed. In order to exploit the full potential of the MIMO system, properly selected signal processing strategies have to be applied. The focus of this work is on the whole testbed functionality including the signal processing needed to separate the data streams. Based on computer simulations the end-to-end functionality of the whole testbed is demonstrated and appropriate quality criteria such as the eye-diagram and the the bit-error rate (BER) are calculated.

The novelty of this paper is given by the proven testbed functionality, which includes the whole electro-optical path with the essential optical MIMO components of mode combining and splitting. The next logical step is the implementation of the MIMO receiver modules such as automatic clock recovery, frame synchronisation, channel estimation and equalisation as demonstrated in [KSD+14].

The remaining part of the paper is structured as follows: In section 2 the optical MIMO testbed and its corresponding system model are introduced. The further processing of the measured impulse responses, which is carried out by inverse filtering, is described in section 3. The obtained results are given in Section 4. Finally, Section 5 shows our concluding remarks.

2 Optical MIMO System Model

An optical MIMO system can be formed by feeding different sources of light into the fibre, which activate different optical mode groups. This can be carried out by using centric and eccentric light launching conditions and subsequent combining of the activated different mode groups with a fusion coupler as show in Fig. 1 [AL13, SAL14]. The different sources

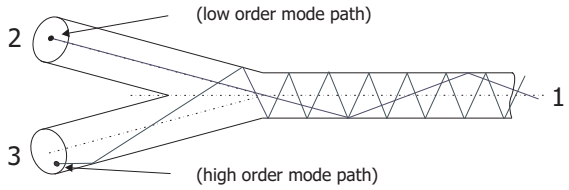


Figure 1: Transmitter side fusion coupler for launching different sources of light into the MMF

of light lead to different power distribution patterns at the fibre end depending on the transmitter side light launch conditions. Fig. 2 highlights the measured mean power distribution pattern at the end of a 1.4 km multi-mode fibre. At the end of the MMF transmission line

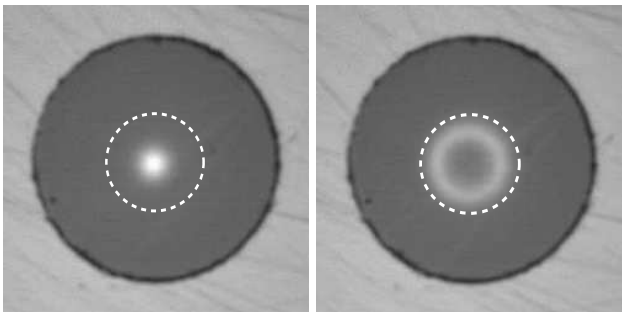


Figure 2: Measured mean power distribution pattern when using the fusion coupler at the transmitter side (left: centric mode excitation; right: eccentric mode excitation); the dotted line represents the $50\,\mu$m core size.

a similar fusion coupler is used for splitting the different mode groups. The measurement setup depicted in Fig. 3 shows the testbed with the utilized devices for measuring the system properties of the optical MIMO channel in form of its specific impulse responses needed for modelling the MIMO data transmission. A picosecond laser unit is chosen for generating the 25 ps input pulse. This input pulse is used to measure separately the different Single-Input Single-Output (SISO) channels within the MIMO system. Since the used picosecond laser unit doesn't guarantee a fully flat frequency spectrum in the region of interest, the captured signals have to be deconvolved. The obtained impulse responses are forming the base for modelling the MIMO transmission system. Fig. 4 highlights the resulting electrical MIMO system model.

3 Measurement Campaign and Signal Deconvolution

Since the process of signal deconvolution is critical in noisy environments, different filtering processes such as Wiener and parametric filtering are studied in order to guarantee a high quality of the deconvolution process defined by the mean square error (MSE) and the imaginary error parameter introduced by Gans [Gan86].

A linear time-invariant system is defined uniquely by its impulse response, or its Fourier transform as the corresponding transfer function. For the determination of the impulse response $g_{\mathrm{k}}(t)$ (see also Fig. 5) an appropriate formed input signal $u_1(t)$ is needed. Unfortunately, an ideal Dirac delta pulse with a frequency independent transfer function is practically not viable. In real systems adequate impulses compared to the Dirac delta pulse must be used. For the determination of the impulse response in optical transmission systems impulses as specified in [ASL13] have proven to be useful. Additionally, when analysing the characteristics of any practical system, the measured impulse $u_3(t)$ is affected by noise. The resulting transmission system model is depicted in Fig. 5. The measured impulse $u_3(t)$ can be decomposed into two parts, namely, the low-pass filtered

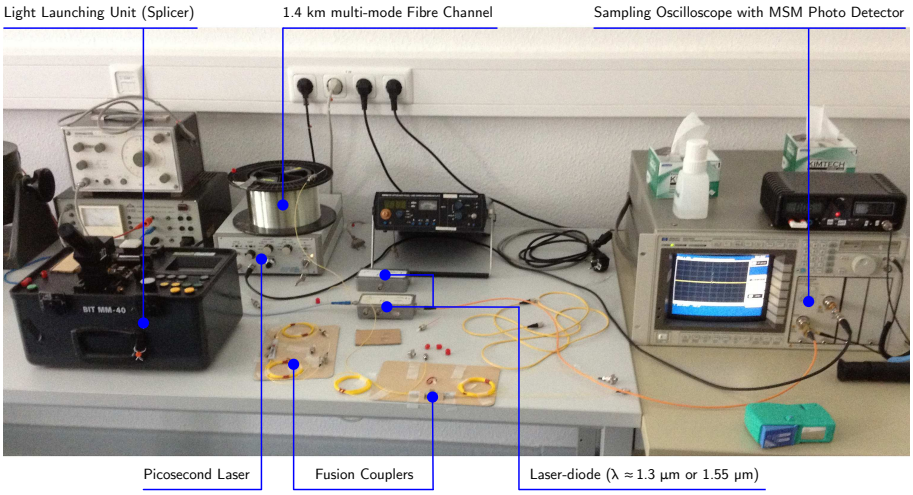


Figure 3: Measurement setup for determining the MIMO specific impulse responses.

output signal $u_2(t)$ and the noise part $n(t)$ resulting in

$$u_3(t) = u_1(t) * g_\mathrm{k}(t) + n(t) \ . \tag{1}$$

In the absence of the noise term, i. e. $n(t) = 0$, the system characteristic $g_\mathrm{k}(t)$ can be easily obtained by inverse filtering and is given as

$$g_\mathrm{k}(t) \quad \circ\!\!-\!\!\bullet \quad G_\mathrm{k}(f) = \frac{U_3(f)}{U_1(f)} \ . \tag{2}$$

Unfortunately, the measured impulse $u_3(t)$ is affected by the noise term $n(t)$. Under these conditions inverse filtering is not working properly anymore. In order to improve the quality of the signal deconvolution different filter functions $h(t)$ are applied and the filtered signal results in

$$u_4(t) = u_1(t) * g_\mathrm{k}(t) * h(t) + n(t) * h(t) \ . \tag{3}$$

This filter operation affects both the low-pass filtered output signal $u_2(t)$ and the noise term $n(t)$. With an appropriate selected filter function the estimation of the impulse response $g_\mathrm{k}(t)$ yields to

$$\hat{g}_\mathrm{k}(t) \quad \circ\!\!-\!\!\bullet \quad \hat{G}_\mathrm{k}(f) = \frac{U_4(f)}{U_1(f)} \ . \tag{4}$$

Hereinafter, two different filter functions types are studied to estimate the impulse response $g_\mathrm{k}(t)$ based on the measured impulse $u_3(t)$. Commonly, the mean square error (MSE) between the impulse response $g_\mathrm{k}(t)$ and the estimated impulse response $\hat{g}_\mathrm{k}(t)$ is chosen as a quality indicator. It is expressed as

$$F_\mathrm{MSE} = \mathrm{E}\{[g_\mathrm{k}(t) - \hat{g}_\mathrm{k}(t)]^2\} \quad \longrightarrow \quad \mathrm{min.} \ , \tag{5}$$

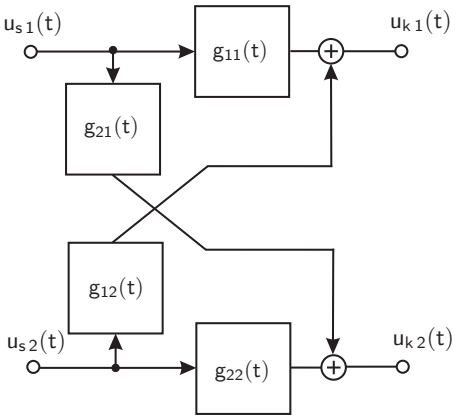


Figure 4: Electrical MIMO system model (example: $n = 2$)

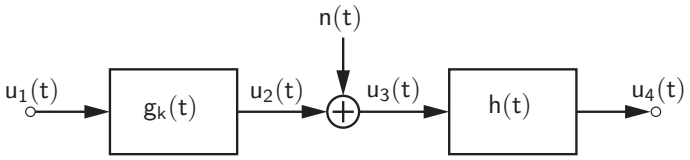


Figure 5: Transmission system model.

where $\mathrm{E}\{\cdot\}$ denotes the expectation functional.

Firstly, the Wiener filter $h_{\mathrm{w}}(t)$ is investigated. It is based on finding the optimal solution for minimizing the MSE when comparing the signal $u_2(t)$ with the filter output signal $u_4(t)$. It is calculated as

$$\mathrm{E}\{[u_2(t) - u_3(t) * h_{\mathrm{w}}(t)]^2\} \quad \longrightarrow \quad \min. \ , \tag{6}$$

Assuming the signal $u_2(t)$ and the noise $n(t)$ are uncorrelated, the Wiener filter transfer function results in [Vas00, pp. 191-194]

$$H_{\mathrm{w}}(f) = \frac{S_{22}(f)}{S_{22}(f) + S_{\mathrm{nn}}(f)} \ , \tag{7}$$

where $S_{22}(f)$ is the power spectral density (PSD) of the signal $u_2(t)$ and $S_{\mathrm{nn}}(f)$ is the noise PSD of the signal $n(t)$.

A more simple filter choice when estimating the impulse response $g_{\mathrm{k}}(t)$ is represented by predefined parametric filter functions. Two one-parametric filters with the transfer function structure

$$H(f) = \frac{|U_1(f)|^2}{|U_1(f)|^2 + \gamma \cdot |X(f)|^2} \ , \qquad \gamma \in \mathbb{R} \tag{8}$$

are analysed. The regularisation filter presented in [NG81] and studied more closely in [SAL13] is given by

$$H_{\mathrm{R}}(f) = H(f) \quad \text{with } X(f) = C(f) \ , \tag{9}$$

where:

$$|C(f)|^2 = 6 - 8\cos(2\pi f T_{\mathrm{a}}) + 2\cos(4\pi f T_{\mathrm{a}}) \tag{10}$$

and T_{a} is the sampling period. The second one-parametric filter described by Nahman and Guillaume is of the same structure and expressed as follows

$$H_{\mathrm{N}}(f) = H(f) \quad \text{with } X(f) = D(f) \ , \tag{11}$$

where:

$$|D(f)|^2 = (2\,\pi\,T_{\mathrm{a}}\,f)^4 \quad . \tag{12}$$

The regularisation filter $H_{\mathrm{R}}(f)$ and the Nahman-Guillaume filter $H_{\mathrm{N}}(f)$ are low-pass filters with the parameter γ influencing the sharpness of the filters and hence determining the cutoff frequencies. The amplitude density spectrum $U_1(f)$ and the γ parameter have the unit Vs. Hereinafter, the unit of γ is not mentioned explicitly. Fig. 6 shows that the transfer function of both filters look consimilar. In order to appropriately select the γ-parameter

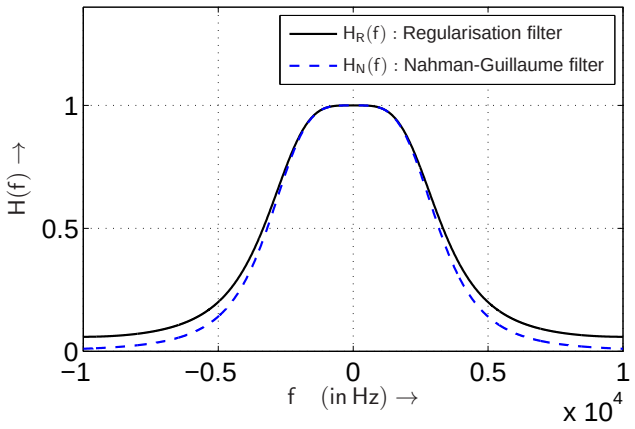


Figure 6: Comparison between the Regularisation filter $H_{\mathrm{R}}(f)$ and the Nahman-Guillaume filter $H_{\mathrm{N}}(f)$ with the parameters $U_1(f) = 1$ Vs, $\gamma = 1$ and $T_{\mathrm{a}} = 50\,\mu$s.

the MSE criterion (5) can be applied for the optimisation. In practical measurements the knowledge of the original impulse response $g_{\mathrm{k}}(t)$ is not given. Therefore, another criterion is needed in order to properly select the γ-parameter for practical measurements. A promising criterion was introduced by Gans [Gan86], where the root mean square of the deconvolved imaginary part of $\hat{g}_{\mathrm{k}}(t)$ is used for finding the parameter of the regularisation function. This optimisation criterion can be expressed as

$$F_{\mathrm{Gans}} = \mathrm{E}\{[\mathrm{Im}\{\hat{g}_{\mathrm{k}}(t,\gamma)\}]^2\} \quad \longrightarrow \quad \min. \ . \tag{13}$$

filter	filter equation	used optimization criterion	signal knowledge necessary	practically applicable
Wiener filter	(7)	$\mathrm{E}\{[u_2(t) - u_3(t) * h_\mathrm{w}(t)]^2\}$	$u_3(t)$, $u_1(t)$, $u_2(t)$	×
$H_\mathrm{R}(f)$ & $H_\mathrm{N}(f)$	(9), (11)	$F_\mathrm{MSE} = \mathrm{E}\{[g_\mathrm{k}(t) - \hat{g}_\mathrm{k}(t)]^2\}$	$u_3(t)$, $u_1(t)$, $g_\mathrm{k}(t)$	×
$H_\mathrm{R}(f)$ & $H_\mathrm{N}(f)$	(9), (11)	$F_\mathrm{Gans} = \mathrm{E}\{[\mathrm{Im}\{\hat{g}_\mathrm{k}(t,\gamma)\}]^2\}$	$u_3(t)$, $u_1(t)$	✓

Table 1: filters and optimisation criteria at a glance

Using this criterion multiple local minima can occur and therefore another criterion described by Nahman and Guillaume in [NG81, pp. 22] should be taken into consideration when choosing the γ value of the regularisation filter. This error criterion is defined as the MSE between the measured receive signal $u_3(t)$ and the simulated receive signal $u_1(t) * \hat{g}_\mathrm{k}(t,\gamma)$, where $u_1(t)$ is the measured input impulse. It is described as follows

$$F_\mathrm{Error}(\gamma) = \mathrm{E}\{[u_3(t) - u_1(t) * \hat{g}_\mathrm{k}(t,\gamma)]^2\} \ . \tag{14}$$

Table 3 gives an overview of all filters and criteria.

In order to compare the quality of the estimated impulse responses using the one-parametric filters to the quality achieved by the Wiener filter, the following system is studied: The input impulse is a Dirac delta pulse with $u_1(t) = U_\mathrm{s}\, T_\mathrm{s}\, \delta(t)$, with $U_s = 1$ V, $T_\mathrm{s} = 1$ ms and $T_\mathrm{s}/T_\mathrm{a} = 20$. The chosen impulse response is

$$g_\mathrm{k}(t) = \frac{1}{T_\mathrm{s}}\ \mathrm{rect}\left(\frac{t}{T_\mathrm{s}}\right) \ . \tag{15}$$

In this case the filter output signal $u_2(t)$ is an rectangular impulse with the amplitude U_s. The deconvolution quality results are depicted in Fig. 7 as a function of the signal-to-noise-ratio E_s/N_0 with the parameter E_s defining the signal energy of $u_2(t)$ and the noise power spectral density N_0 of the signal $n(t)$. When applying the one-parametric filters $H_\mathrm{R}(f)$ and $H_\mathrm{N}(f)$ the optimal γ values as well as the MSE are decreasing with increasing E_s/N_0. The achievable quality of the estimated impulse responses using the one-parametric filters together with the MSE optimisation criterion is nearly identical and comes close to the Wiener filter results. The benefit of using a filter function is clearly visible.

In order to determine the quality of the estimated impulse responses, which are practically obtainable using the Gans' criterion (13), the following optical system configuration is studied: The measured input impulse of the picosecond laser is depicted in Fig. 8 for different operating wavelengths with a pulse width of approximately 25 ps. For the following simulation the operating wavelength is chosen to be 1576 nm. The impulse response is carried out as a first-order low pass filter and is described as follows

$$G_\mathrm{k}(f) = A \cdot \frac{1}{1 + \mathrm{j}\, 2\, \pi\, f\, T_1} \ , \tag{16}$$

where $T_1 = T_\mathrm{s} = 0.8$ ns and $T_\mathrm{s}/T_\mathrm{a} = 200$. The scaling factor A is chosen to maintain $E_s/T_s = 1\,\mathrm{V}^2$ of the signal $u_2(t)$ and to ensure the unit s^{-1} of the impulse response. Fig. 9 shows the quality of the obtained impulse responses using the filter functions mentioned before. The regularisation filter and the Nahman-Guillaume filter are applied for

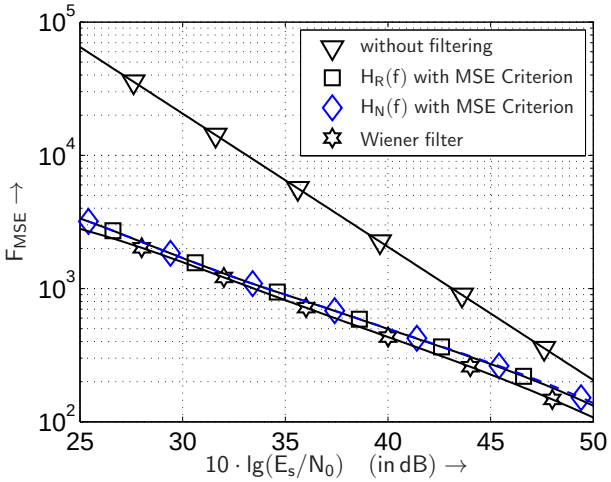


Figure 7: Quality F_{MSE} of the deconvolved impulse responses as a function of signal energy to noise power spectral density using different filter functions.

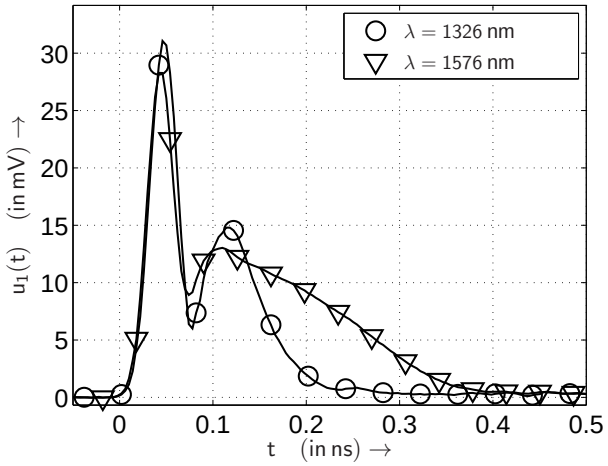


Figure 8: Measured input impulses at different operating wavelengths λ.

both optimisation criteria resulting in γ values depicted in Fig. 10. The γ values are also decreasing with increasing E_{s}/N_0 for both criteria. It should be noted, that the γ values using the Gans' criterion are lower compared to the MSE criterion. This signifies that the measured signal $u_3(t)$ is filtered less when applying the filter using the Gans' criterion in contrast to using the MSE criterion. As expected, the deconvolved impulse responses

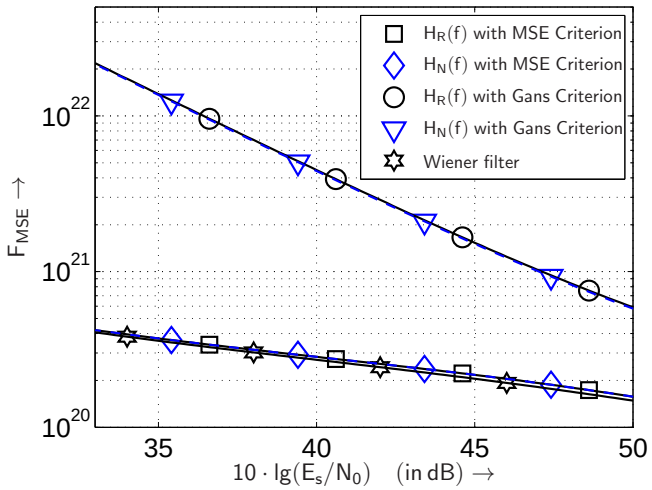


Figure 9: Quality F_{MSE} of the deconvolved impulse responses as a function of signal energy to noise power spectral density using different filters.

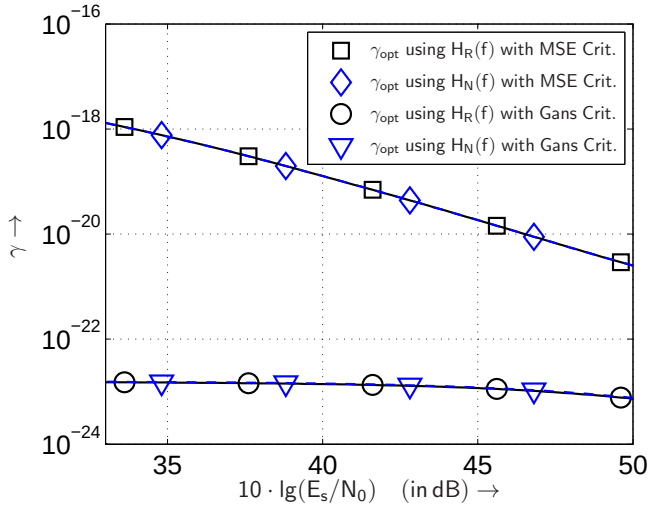


Figure 10: Choice of optimal γ when filtering with the regularisation filter $H_{\mathrm{R}}(f)$ and the Nahman-Guillaume filter $H_{\mathrm{N}}(f)$ minimizing the MSE and using the Gans' criterion.

using the Wiener filter are showing the best quality of all applied filter functions closely followed by the estimated impulse responses filtered with the one-parametric filters using the MSE optimisation criterion. The quality of the estimated impulse responses using

the Gans' criterion is still acceptable for a wide range of E_s/N_0 values and is a major improvement comparing to the quality without filtering (not depicted). The obtained results show further that both parametric filters, whose quality is nearly identical, are a good compromise compared to the Wiener filter with its high complexity.

Applying the described deconvolution processing to the (2×2) MIMO testbed, the obtained impulse responses are depicted in Fig. 11-12. They are calculated by applying the regularisation filter in the deconvolution process with γ values respecting the Gans' and Error criterion. At an operating wavelength of 1326 nm the modal structure can be identi-

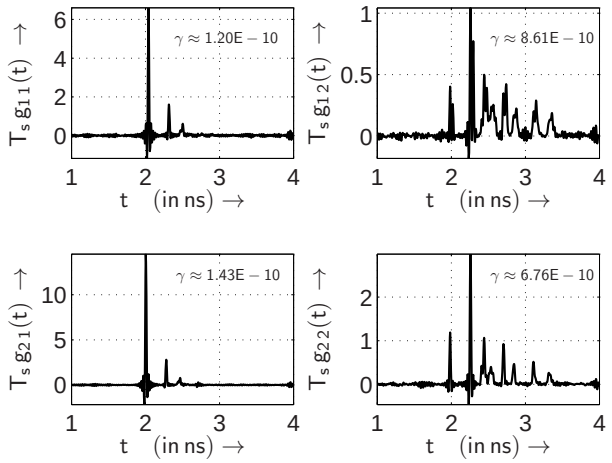


Figure 11: Deconvolved measured electrical MIMO impulse responses with respect to the pulse frequency $f_\mathrm{T} = 1/T_\mathrm{s} = 620$ MHz at 1326 nm operating wavelength using the regularisation filter function with γ values according to the Gans' criterion.

fied. Considering the 1576 nm results the additional influence of the chromatic dispersion is clearly visible.

4 MIMO Equalisation and Simulation Results

In this section the MIMO baseband transmission system is constructed as illustrated in Fig. 13. It uses the deconvolved (2×2) MIMO specific impulse responses $g_{i,j}(t)$ (for $i = 1, 2$ and for $j = 1, 2$) depicted in Fig. 12 at 1576 nm operating wavelength. In this baseband system model the transmitter forms a rectangular pulse train and hence the transmit filter $g_\mathrm{s}(t)$ and the receive filter $g_\mathrm{ef}(t)$ are considered to be matched filters and are described in its non causal notation with

$$g_\mathrm{s}(t) = g_\mathrm{ef}(t) = \frac{1}{T_\mathrm{s}} \, \mathrm{rect}\left(\frac{t}{T_\mathrm{s}}\right) \quad . \tag{17}$$

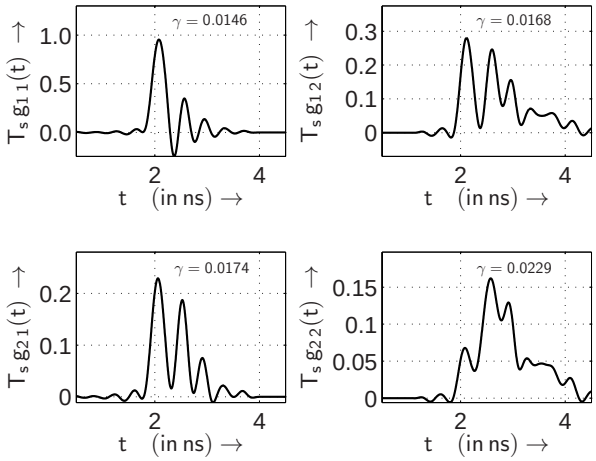


Figure 12: Deconvolved measured electrical MIMO impulse responses with respect to the pulse frequency $f_\mathrm{T} = 1/T_\mathrm{s} = 620$ MHz at 1576 nm operating wavelength using the regularisation filter function with γ values according to the Gans' criterion.

The total transmit power is normalised to $P_\mathrm{s} = 1\,\mathrm{V}^2$ and a symbol pulse frequency of $f_\mathrm{T} = 1/T_\mathrm{s} = 620$ MHz per data channel is used resulting in a total bit rate of 1.24 Gb/s for both channels. Both transmit signals $u_{\mathrm{s},j}(t)$ are launched onto the (2×2) MIMO channel. The filtered receive signals $u_{\mathrm{e},i}(t)$ are sampled with kT_s, where $k \in \mathbb{Z}$. The system can be simplified by introducing the cumulative channel impulse response $h_{i,j}(t)$ and the filtered noise $w_i(t)$ expressed as follows

$$\begin{aligned} h_{i,j}(t) &= g_\mathrm{s}(t) * g_{i,j}(t) * g_\mathrm{ef}(t), \qquad & h_{i,j}(k) &= h_{i,j}(t)\Big|_{kT_\mathrm{s}} \\ w_i(t) &= n_i(t) * g_\mathrm{ef}(t), & w_i(k) &= w_i(t)\Big|_{kT_\mathrm{s}} \end{aligned} \tag{18}$$

By utilising a data block transmission model [RC98, RJ99] a vectorial notation can be applied as follows

$$\begin{aligned} \boldsymbol{c} &= \begin{pmatrix} c[1] & c[2] & \cdots & c[K] \end{pmatrix}^\mathrm{T} \\ \boldsymbol{h}_{i,j} &= \begin{pmatrix} h_{i,j}[1] & h_{i,j}[2] & \cdots & h_{i,j}[L] \end{pmatrix}^\mathrm{T} \quad . \end{aligned} \tag{19}$$

Using the convolution matrices $\boldsymbol{H}_{i,j}$ the transmission model can be described as

$$\begin{aligned} \boldsymbol{u}_1 &= \boldsymbol{H}_{11} \cdot \boldsymbol{c}_1 + \boldsymbol{H}_{12} \cdot \boldsymbol{c}_2 + \boldsymbol{w}_1 \\ \boldsymbol{u}_2 &= \boldsymbol{H}_{21} \cdot \boldsymbol{c}_1 + \boldsymbol{H}_{22} \cdot \boldsymbol{c}_2 + \boldsymbol{w}_2 \quad . \end{aligned} \tag{20}$$

Written in matrix notation

$$\begin{pmatrix} \boldsymbol{u}_1 \\ \boldsymbol{u}_2 \end{pmatrix} = \begin{pmatrix} \boldsymbol{H}_{11} & \boldsymbol{H}_{12} \\ \boldsymbol{H}_{21} & \boldsymbol{H}_{22} \end{pmatrix} \cdot \begin{pmatrix} \boldsymbol{c}_1 \\ \boldsymbol{c}_2 \end{pmatrix} + \begin{pmatrix} \boldsymbol{w}_1 \\ \boldsymbol{w}_2 \end{pmatrix} \quad . \tag{21}$$

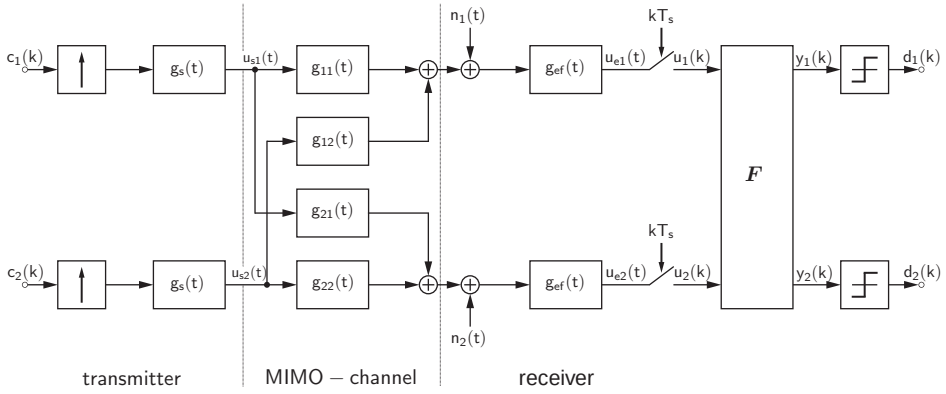


Figure 13: (2×2) MIMO baseband transmission system model with discrete zero–forcing equaliser.

Simplifying this equation results in

$$\boldsymbol{u} = \boldsymbol{H} \cdot \boldsymbol{c} + \boldsymbol{w} \ , \tag{22}$$

where the channel matrix $\boldsymbol{H}$ contains the ISI as well as the crosstalk information. For obtaining the transmitted symbols unaffected from the channel

$$\boldsymbol{F} \cdot \boldsymbol{H} = \boldsymbol{I} \tag{23}$$

has to be fulfilled, where $\boldsymbol{I}$ is a identity matrix and thus the equaliser matrix $\boldsymbol{F}$ can be obtained as follows

$$\boldsymbol{F} = (\boldsymbol{H}^{\mathrm{H}}\, \boldsymbol{H})^{-1} \boldsymbol{H}^{\mathrm{H}} \quad . \tag{24}$$

Hereinafter, the equaliser matrix $\boldsymbol{F}$ is applied to the received data vector $\boldsymbol{u}$

$$\begin{aligned} \boldsymbol{y} &= \boldsymbol{F} \cdot \boldsymbol{u} \\ \boldsymbol{y} &= \boldsymbol{c} + \boldsymbol{F} \cdot \boldsymbol{w} \ . \end{aligned} \tag{25}$$

The benefit of applying this zero–forcing (ZF) equaliser is the orthogonalisation of the transmission channels. Thus, the resulting equalised MIMO system can be described by two independent SISO channels. The disadvantage of using the ZF equaliser is the weighting of the noise term.

Eye diagrams of both received signals in the MIMO system after equalisation are shown in Fig. 14. Using the ZF equaliser both eyes are fully opened confirming its functionality. The MIMO bit-error rate (BER) simulation results are depicted in Fig. 15 and underline the functionality of the equaliser.

5 Conclusion

In this contribution a (2×2) optical MIMO communication system, consisting of a 1.4 km multi-mode fibre and optical couplers attached to both ends, has been analysed. The

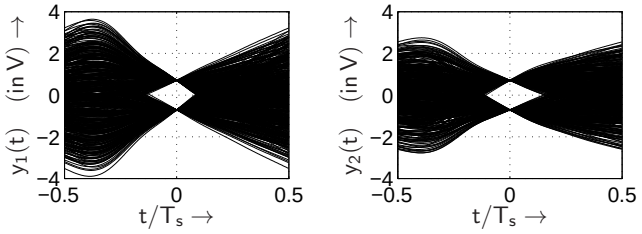


Figure 14: Eye diagram patterns of both received signals when applying zero–forcing equalisation.

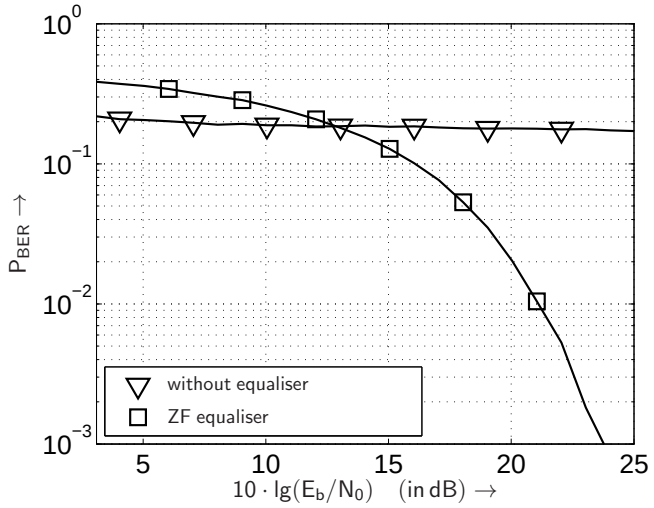


Figure 15: (2×2) MIMO BER probability as a function of bit energy E_b to noise PSD with and without applying the zero–forcing equalising method using the deconvolved MIMO impulse responses at 1576 nm operating wavelength and transmitting with a bit rate of 1.24 Gb/s.

estimations of the MIMO specific impulse responses have been obtained for operating wavelengths of 1576 nm and 1326 nm using optimized signal deconvolution by applying the parametric regularisation filter. It has been shown that the quality of the estimated impulse responses significantly improves and is comparable to Wiener filtering. These estimated impulse responses have been used for modelling a baseband MIMO data transmission system. In order to receive the transmitted data unaffected from the data send on the neighbouring channel zero–forcing equalisation has been investigated. The successful implementation has been shown by the bit-error curves as well as by the open eye-diagram.

References

[AL13] A. Ahrens and S. Lochmann. Optical Couplers in Multimode MIMO Transmission Systems: Measurement Results and Performance Analysis. In *International Conference on Optical Communication Systems (OPTICS)*, pages 398–403, Reykjavik (Iceland), 29.–31. July 2013.

[ASL13] A. Ahrens, A. Schröder, and S. Lochmann. Dispersion Analysis within a Measured 1,4 km MIMO Multimode Channel. In *International Conference on Optical Communication Systems (OPTICS)*, pages 391–397, Reykjavik (Island), 29.–31. July 2013.

[Gan86] W. L. Gans. Calibration and Error Analysis of a Picosecond Pulse Waveform Measurement System at NBS. *Proceedings of the IEEE*, 74(1):86–90, January 1986.

[KÖ6] V. Kühn. *Wireless Communications over MIMO Channels – Applications to CDMA and Multiple Antenna Systems.* Wiley, Chichester, 2006.

[KSD+14] H. Köhnke, R. Schwinkendorf, S. Daase, A. Ahrens, and S. Lochmann. Receiver Design for an Optical MIMO Testbed. In *International Conference on Optical Communication Systems (OPTICS)*, pages 31–36, Vienna (Austria), 28.–30. August 2014.

[NG81] N. S. Nahman and M. E. Guillaume. *Deconvolution of Time Domain Waveforms in the Presence of Noise*. National Bureau of Standards Technical Note 1047, Boulder, Colorado 80303, October 1981.

[RC98] G. G. Raleigh and John M. Cioffi. Spatio-Temporal Coding for Wireless Communication. *IEEE Transactions on Communications*, 46(3):357–366, March 1998.

[RFN13] D. J. Richardson, J.M. Fini, and L.E. Nelson. Space Division Multiplexing in Optical Fibres. *Nature Photonics*, 7:354–362, 2013.

[RJ99] G. G. Raleigh and V. K. Jones. Multivariate Modulation and Coding for Wireless Communication. *IEEE Journal on Selected Areas in Communications*, 17(5):851–866, May 1999.

[SAL13] A. Sandmann, A. Ahrens, and S. Lochmann. Signal Deconvolution of Measured Optical MIMO-Channels. In *XV International PhD Workshop OWD 2013*, pages 278–283, Wisła, Poland, 19.–22. October 2013.

[SAL14] A. Sandmann, A. Ahrens, and S. Lochmann. Experimental Description of Multimode MIMO Channels utilizing Optical Couplers. In *15. ITG-Fachtagung Photonische Netze – ITG-Fachbericht Band 248*, pages 125–130, Leipzig (Germany), 05.–06. May 2014.

[SSB08] A. C. Singer, N. R. Shanbhag, and Hyeon-Min Bae. Electronic Dispersion Compensation – An Overwiew of Optical Communications Systems. *IEEE Signal Processing Magazine*, 25(6):110–130, 2008.

[TV05] D. Tse and P. Viswanath. *Fundamentals of Wireless Communication*. Cambridge, New York, 2005.

[Vas00] Saeed Vaseghi. *Advanced Digital Signal Processing and Noise Reduction, Second Edition*. John Wiley & Sons Ltd, Chichester, 2000.

[Win12] P. J. Winzer. Optical Networking beyond WDM. *IEEE Photonics Journal*, 4:647–651, 2012.

Resource Allocation Strategies in SVD-equalized Broadband MIMO Systems

Ahmed Mamdouh El-Shafiey, Francisco Cano-Broncano, Andreas Ahrens.
Cairo University, Faculty of Engineering.
Universidad Politcnica de Madrid.
Hochschule Wismar University of Technology, Business and Design.
email: ahmed.mamdouh.elshafiey@gmail.com, francisco.cano.broncano@gmail.com,
andreas.ahrens@hs-wismar.de.

Abstract: Adaptive bit and power allocation schemes in broadband Multiple-Input Multiple-Output (MIMO) systems are generally aiming to maximize the overall system throughput. However, in delay-critical applications such as voice or video streaming, a fixed data rate is crucial. Therefor in this contribution, bit and power allocation schemes in broadband MIMO systems for fixed rate applications are developed. The proposed schemes aim for optimizing the number of active MIMO layers and the number of bits per symbol in addition to an appropriate power assignment. The main goal is to minimize the overall bit-error rate (BER) for a given fixed data rate and limited transmit power. It turned out that it is not necessary to activate all MIMO layers in order to optimize the BER performance. Moreover, it can be seen from computer simulation results that multipath propagation is not a limiting factor in broadband MIMO systems.

1 Introduction

By exploiting the spatial dimension with systems composed of multiple transmit and receive antennas, also called MIMO systems, the spectral efficiency can be widely improved compared to the conventional Single-Input Single-Output (SISO) systems [ZT03, BZBO13]. Therefore, MIMO communication architecture has become crucial in future high-rate wireless applications. In systems with perfect channel state information (PCSI), further improvements to the system throughput can be achieved by adapting the system parameters to the varying channel state information, i.e., implementing adaptive modulation (AM) technique [AG99]. Combining MIMO system architecture with AM techniques, the performance of the system can be enhanced considerably [RR02, GD05]. However, in real-time interactive applications, a fixed data rate is more preferable in comparison with system throughput improvements. Therefore, it is necessarily demanded to develop adaptive bit and power allocation schemes which optimize the BER performance for a given fixed data rate. Bit auctioning and power assignment strategies have attracted high attention in frequency non-selective MIMO systems and reached a state of maturity [AL08]. By contrast, bit and power allocation schemes in broadband MIMO systems require further substantial research.

In order to minimize the overall MIMO system BER, additional degrees of freedom are introduced by employing adaptive resource allocation schemes. However, the system-inherited interference such as inter-antenna interference and inter-symbol interference (ISI), introduced by the frequency selective channel, tends to decrease the overall system BER performance. Thus it requires appropriate handling. A popular signal processing strategy based on Singular Value Decomposition (SVD) has been widely used to resolve the overall interference in broadband MIMO systems [AL08, ABP09, AABP10]. Regarding this background, the novel contribution of this paper is to investigate the efficiency of implementing bit and power allocation schemes for SVD-equalized broadband MIMO systems with PCSI. The proposed adaptive schemes aim for achieving optimized BER performance while maintaining fixed data throughput and limited total power.

The remaining part of this paper is organized as follows: Section 2 presents the broadband MIMO system model. The proposed quality criteria including the BER analysis of the investigated MIMO system is reviewed in Section 3. Bit and power loading techniques are developed in Section 4. Simulation results concerning the system performance are obtained and interpreted in Section 5. Finally, Section 6 provides some concluding remarks.

2 Broadband MIMO System Model

In this section the discrete time model for broadband MIMO system is presented. The investigated MIMO system architecture is composed of n_{T} transmit antennas at the transmitter side and n_{R} receive antennas at the receiver side. The frequency selective channel is considered to have $(L_{\mathrm{c}}+1)$ channel paths, i.e., the effective length of the channel's finite impulse response (FIR). Therefore, the input-output discrete-time formulation for broadband MIMO system is given by

$$u_{\nu}[k] = \sum_{\mu=1}^{n_{\mathrm{T}}} \sum_{\kappa=0}^{L_{\mathrm{c}}} h_{\nu,\mu}[\kappa] \cdot c_{\mu}[k-\kappa] + n_{\nu}[k], \tag{1}$$

where $u_{\nu}[k]$ is the received symbol at the νth receive antenna (with $\nu = 1, 2, \ldots, n_{\mathrm{R}}$), $c_{\mu}[k]$ is the transmitted symbol from the μth transmit antenna (with $\mu = 1, 2, \ldots, n_{\mathrm{T}}$) and $n_{\nu}[k]$ is the Additive White Gaussian Noise (AWGN) at the νth receive antenna having zero mean and variance U_{R}^2. The parameter k is the discrete time index. The channel influence between the μth transmit antenna and the νth receive antenna is represented by the channel coefficients $h_{\nu,\mu}[\kappa]$ (with $\kappa = 0, 1, \ldots, L_{\mathrm{c}}$), i.e., the channel weightings arising at the κth channel paths. The FIR of the channel, denoted by the channel coefficients, includes the effect of transmit and receive filtering as well as the multipath component introduced by the channel [LXG02]. Additionally, throughout this paper, the channel coefficients are assumed to undergo a Rayleigh distribution and have the same average power.

In the following analysis, block data transmission model is employed, by which K data symbols are grouped to form a data block. Afterwards, the data blocks are separated by synchronization symbols. Furthermore, a block fading model is applied, i.e., the channel is

assumed to be time-invariant for the duration of a complete data block. By expanding (1) to take into account $(K + L_{\mathrm{c}})$ consecutive received symbols at each receive antenna, i.e., applying the block data transmission model, the block-oriented model of the broadband MIMO system results in

$$\mathbf{u}_{\nu} = \sum_{\mu=1}^{n_{\mathrm{T}}} \mathbf{H}_{\nu,\mu} \cdot \mathbf{c}_{\mu} + \mathbf{n}_{\nu} \,, \tag{2}$$

where u_{ν} is the $((K + L_{\mathrm{c}}) \times 1)$ received symbol vector at the νth receive antenna and is defined as

$$\mathbf{u}_{\nu} = \left[\; u_{\nu}\left[1\right], \quad u_{\nu}\left[2\right], \quad \ldots, \quad u_{\nu}\left[K + L_{\mathrm{c}}\right] \; \right]^{\mathrm{T}} \cdot \tag{3}$$

The $((K + L_{\mathrm{c}}) \times K)$ channel matrix $\mathbf{H}_{\nu,\mu}$ is the SISO channel influence between the μth transmit antenna and the νth receive antenna through the complete data block. Considering (1), the channel matrix $\mathbf{H}_{\nu,\mu}$ is according to

$$\mathbf{H}_{\nu,\mu} = \begin{bmatrix} h_{\nu,\mu}\left[0\right] & 0 & \cdots & 0 & 0 \\ h_{\nu,\mu}\left[1\right] & h_{\nu,\mu}\left[0\right] & \ddots & \vdots & \vdots \\ \vdots & h_{\nu,\mu}\left[1\right] & \ddots & 0 & \vdots \\ h_{\nu,\mu}\left[L_{\mathrm{c}}\right] & \vdots & \ddots & h_{\nu,\mu}\left[0\right] & 0 \\ 0 & h_{\nu,\mu}\left[L_{\mathrm{c}}\right] & \cdots & h_{\nu,\mu}\left[1\right] & h_{\nu,\mu}\left[0\right] \\ \vdots & \ddots & \ddots & \vdots & h_{\nu,\mu}\left[1\right] \\ 0 & \cdots & 0 & h_{\nu,\mu}\left[L_{\mathrm{c}}\right] & \vdots \\ 0 & \cdots & \cdots & 0 & h_{\nu,\mu}\left[L_{\mathrm{c}}\right] \end{bmatrix} . \tag{4}$$

The $(K \times 1)$ vector c_{μ} denotes the transmit symbol vector from the μth transmit antenna, i.e., the transmit data block and is modeled by

$$\mathbf{c}_{\mu} = \left[\; c_{\mu}\left[1\right], \quad c_{\mu}\left[2\right], \quad \ldots, \quad c_{\mu}\left[K\right] \; \right]^{\mathrm{T}} \cdot \tag{5}$$

The $((K + L_{\mathrm{c}}) \times 1)$ vector n_{ν} represents the AWGN at the νth receive antenna and is given by

$$\mathbf{n}_{\nu} = \left[\; n_{\nu}\left[1\right], \quad n_{\nu}\left[2\right], \quad \ldots, \quad n_{\nu}\left[K + L_{\mathrm{c}}\right] \; \right]^{\mathrm{T}} \cdot \tag{6}$$

The block-oriented system model described in (2) is expanded to include n_R receive antennas at the receiver side and results in

$$\begin{bmatrix} \mathbf{u}_1 \\ \mathbf{u}_2 \\ \vdots \\ \mathbf{u}_{n_{\mathrm{R}}} \end{bmatrix} = \begin{bmatrix} \mathbf{H}_{1,1} & \cdots & \mathbf{H}_{1,n_{\mathrm{T}}} \\ \vdots & \ddots & \vdots \\ \mathbf{H}_{n_{\mathrm{R}},1} & \cdots & \mathbf{H}_{n_{\mathrm{R}},n_{\mathrm{T}}} \end{bmatrix} \cdot \begin{bmatrix} \mathbf{c}_1 \\ \mathbf{c}_2 \\ \vdots \\ \mathbf{c}_{n_{\mathrm{T}}} \end{bmatrix} + \begin{bmatrix} \mathbf{n}_1 \\ \mathbf{n}_2 \\ \vdots \\ \mathbf{n}_{n_{\mathrm{R}}} \end{bmatrix} , \tag{7}$$

which can be written as

$$\mathbf{u} = \mathbf{H} \cdot \mathbf{c} + \mathbf{n} \cdot \tag{8}$$

The channel matrices $\mathbf{H}_{\nu,\mu}$ introduce ISI between neighboring symbols as well as the interference introduced by the different antenna data streams. To eliminate this interference, as investigated in the literature [AL08, ABP09], a popular signal processing technique based on SVD is applied, by which the overall MIMO channel matrix is written as $\mathbf{H} = \mathbf{S} \cdot \mathbf{V} \cdot \mathbf{D}^{\mathrm{H}}$. Such that $\mathbf{S}$ and $\mathbf{D}$ are unitary matrices composed of the eigenvectors of $\mathbf{H}\mathbf{H}^{\mathrm{H}}$ and $\mathbf{H}^{\mathrm{H}}\mathbf{H}$ respectively, with $(\cdot)^{\mathrm{H}}$ denoting the conjugate transpose operator. The matrix $\mathbf{V}$ is a rectangular diagonal matrix having $\left(\sqrt{\xi_1}, \sqrt{\xi_2}, ..., \sqrt{\xi_{n_{\mathrm{S}}}}\right)$ on its main diagonal arranged in descending order (with $n_{\mathrm{S}} \leq K \cdot \min\left(n_{\mathrm{R}}, n_{\mathrm{T}}\right)$ per MIMO data block). The singular values $\sqrt{\xi_i}$ are the square roots of the ith positive eigenvalues (with $i = 1, 2, \ldots, n_{\mathrm{s}}$) of $\mathbf{H}\mathbf{H}^{\mathrm{H}}$ or $\mathbf{H}^{\mathrm{H}}\mathbf{H}$. Applying SVD on the system requires signal preprocessing at the transmitter side as well as signal post processing at the receiver side. Such that at the transmitter the MIMO transmitted data block is multiplied by $\mathbf{D}$ and at the receiver the MIMO received data block is multiplied by $\mathbf{S}^{\mathrm{H}}$. Upon applying SVD signal processing, the block-oriented system model results in

$$\begin{aligned} \mathbf{y} &= \mathbf{S}^{\mathrm{H}} \cdot (\mathbf{H} \cdot \mathbf{D} \cdot \mathbf{c} + \mathbf{n}) \\ \mathbf{y} &= \mathbf{S}^{\mathrm{H}} \cdot \mathbf{S} \cdot \mathbf{V} \cdot \mathbf{D}^{\mathrm{H}} \cdot \mathbf{D} \cdot \mathbf{c} + \mathbf{S}^{\mathrm{H}} \cdot \mathbf{n} \\ \mathbf{y} &= \mathbf{V} \cdot \mathbf{c} + \mathbf{w} \cdot \end{aligned} \tag{9}$$

The vector $\mathbf{y}$ denotes the received symbol vector including all n_R receive antennas after applying SVD, the vector $\mathbf{c}$ is the transmit symbol vector from all n_T transmit antennas and the vector $\mathbf{w}$ is the AWGN vector at all n_R receive antennas multiplied by $\mathbf{S}^{\mathrm{H}}$. Upon applying SVD signal processing, the off-diagonal elements in the overall channel matrix $\mathbf{H}$ are eliminated, thus the inter-antenna interference as well as the ISI are eliminated. Moreover, the overall MIMO channel matrix $\mathbf{H}$ is converted into independent non-interfering layers of unequal weightings. This results in different noise immunity per each MIMO layer which requires appropriate handling. Thus to minimize the overall BER for a given fixed data rate, employing layer-specific bit and power allocation schemes is recommended.

3 Quality Criteria

The BER for M-ary Quadrature Amplitude Modulation (QAM) systems over AWGN channel, according to [ABP09, VPL10], is calculated as follows

$$P_{\mathrm{BER}} = \frac{2}{\log_2(M)} \left(1 - \frac{1}{\sqrt{M}}\right) \operatorname{erfc}\left(\sqrt{\frac{\rho}{2}}\right), \tag{10}$$

where M is the number of symbols in QAM constellation. The parameter ρ denotes the signal-to-noise ratio (SNR) and is defined as $\rho = {}^{U_{\mathrm{A}}^2}/_{U_{\mathrm{R}}^2}$, such that U_{A} is the half vertical eye opening and U_{R}^2 is the AWGN power per quadrature component. Upon Introducing the proposed SVD-equalized MIMO system model, the layer-specific half vertical eye opening at time slot k (with $k = 1, 2, \ldots, K$) results in

$$U_{\mathrm{A}}^{(\ell,k)} = \sqrt{\xi_{\ell,k}} \cdot U_{\mathrm{s}\,\ell}\,, \tag{11}$$

where $U_{s\,\ell}$ is the half level transmit amplitude for layer ℓ (with $\ell = 1, 2, \ldots, L$), and the parameter L describes the number of active MIMO layers, i.e., $L \leq \min(n_{\mathrm{T}}, n_{\mathrm{R}})$ for parallel transmission. The singular value $\sqrt{\xi_{\ell,k}}$ represents the gain of the ℓth MIMO layer at time slot k. The average power in M-ary QAM constellation is written in terms of the half level transmit amplitude as follow [ABP09, VPL10]

$$P_{\mathrm{s}\,\ell} = \frac{2}{3} U_{\mathrm{s}\,\ell}^2 \left(M_\ell - 1\right) , \tag{12}$$

where $P_{\mathrm{s}\,\ell}$ is the average assigned power in M-ary QAM constellation of the ℓth MIMO layer. Assuming the total power P_{s} is divided equally on all active layers L. The power allocated to each MIMO layer $P_{\mathrm{s}\,\ell}$ results in

$$P_{\mathrm{s}\,\ell} = \frac{P_{\mathrm{s}}}{L} \cdot \tag{13}$$

where the total transmit power P_{s} provided to the MIMO system is defined as

$$P_{\mathrm{s}} = \sum_{\ell=1}^{L} P_{\mathrm{s}\,\ell} \cdot \tag{14}$$

Combining (11), (12) and (13) the layer-specific SNR is according to

$$\rho^{(\ell,k)} = \xi_{\ell,k} \cdot \frac{U_{\mathrm{s}\,\ell}^2}{U_{\mathrm{R}}^2} = \frac{3}{2} \frac{\xi_{\ell,k} \cdot P_{\mathrm{s}}}{L\left(M_\ell - 1\right) U_{\mathrm{R}}^2} \cdot \tag{15}$$

Given (10) and (15), the BER for the ℓth MIMO layer at time slot k results in

$$P_{\mathrm{BER}}^{(\ell,k)} = \frac{2\left(1 - \frac{1}{\sqrt{M_\ell}}\right)}{\log_2\left(M_\ell\right)} \operatorname{erfc}\left(\sqrt{\frac{3\,\xi_{\ell,k}}{4\,L\left(M_\ell - 1\right)} \frac{P_{\mathrm{s}}}{U_{\mathrm{R}}^2}}\right) . \tag{16}$$

Taking into account all active MIMO layers, the average BER at time slot k is obtained as

$$P_{\mathrm{BER}}^{(k)} = \frac{1}{\sum\limits_{\nu=1}^{L} \log_2\left(M_\nu\right)} \sum_{\ell=1}^{L} \log_2\left(M_\ell\right) \cdot P_{\mathrm{BER}}^{(\ell,k)} \cdot \tag{17}$$

Finally the average BER per MIMO data block P_{BER} is according to

$$P_{\mathrm{BER}} = \frac{1}{K} \sum_{k=1}^{K} P_{\mathrm{BER}}^{(k)} \cdot \tag{18}$$

By taking different channel SNR into account, the overall BER performance can be evaluated. As described in (17) and (18), the average BER per complete data block P_{BER} is dominated by the transmission mode employed in each of the active MIMO layers, i.e., the assigned QAM constellations. Therefore, different transmission modes results in different BERs. The transmission modes tabulated in Tab. 1 for (4×4) MIMO systems with fixed data throughput of 8 bit/s/Hz are investigated. It is required to find out the best combination of QAM modes and number of activated MIMO layers which optimizes the BER performance.

Table 1: Investigated QAM transmission modes for fixed transmission bit rate

throughput	layer 1	layer 2	layer 3	layer 4
8 bit/s/Hz	4	4	4	4
8 bit/s/Hz	**16**	**4**	**4**	**0**
8 bit/s/Hz	**16**	**16**	**0**	**0**
8 bit/s/Hz	**64**	**4**	**0**	**0**
8 bit/s/Hz	256	0	0	0

4 Bit and Power Loading Techniques

Considering that the average BER at each time slot is obtained by the BER performance of each of the active MIMO layers. Thus, Power Allocation (PA) strategy can be employed to enhance the overall BER performance, such that an appropriate power level is assigned to each active MIMO layer. The PA strategy multiplies the layer-specific half level transmit amplitude $U_{\mathrm{s}\ell}$ with a time-varying layer-specific factor $\sqrt{p_{\ell,k}}$. The aim of the upcoming analysis is to derive the values of $\sqrt{p_{\ell,k}}$ which fulfill the main goal of the PA strategy, i.e., optimal or nearly optimal BER performance. The calculation of the optimal values of $\sqrt{p_{\ell,k}}$, which results in the optimal BER performance, involves using Lagrange multiplier method [AL08, PL04]. Thus excessive complexity optimization problem is introduced. Therefore, sub-optimal PA strategies with lower complexities are of common interest [ABP09, AABP10, PL04]. The layer with the lowest SNR provides the worst impact on the average BER. Therefore, a natural choice is to assign different power levels to each active MIMO layer in a way that an equal-SNR in all active layers is guaranteed at each time slot. Upon applying equal-SNR PA strategy, the half vertical eye opening results in

$$U_{\mathrm{A\,PA}}^{(\ell,k)} = \sqrt{p_{\ell,k}} \cdot \sqrt{\xi_{\ell,k}} \cdot U_{\mathrm{s}\,\ell}\,. \tag{19}$$

The layer-specific SNR after the PA strategy is obtained as

$$\rho_{\mathrm{PA}}^{(\ell,k)} = \frac{\left(U_{\mathrm{A\,PA}}^{(\ell,k)}\right)^2}{U_{\mathrm{R}}^2} = p_{\ell,k} \cdot \rho^{(\ell,k)}\,, \tag{20}$$

where $\rho_{\mathrm{PA}}^{(\ell,k)}$ is guaranteed to be constant for $\ell = 1, 2, \ldots, L$. The total transmit power restriction in the PA strategy is given by

$$P_{\mathrm{s}} = \sum_{\ell=1}^{L} P_{\mathrm{s}\ell} \cdot p_{\ell,k} = \frac{P_{\mathrm{s}}}{L} \cdot \sum_{\ell=1}^{L} p_{\ell,k}\,. \tag{21}$$

Given (15), (20) and (21), it can be shown that the time-varying layer-specific PA factors are calculated as follows [AL08]

$$p_{\ell,k} = \frac{L\ (M_\ell - 1)}{\xi_{\ell,k} \sum\limits_{\nu=1}^{L} \frac{(M_\nu - 1)}{\xi_{\nu,k}}} \cdot \tag{22}$$

The updated layer-specific SNR results in

$$\rho_{\mathrm{PA}}^{(\ell,k)} = \frac{3\,P_{\mathrm{s}}}{2\,U_{\mathrm{R}}^2} \cdot \frac{1}{\sum\limits_{\nu=1}^{L} \frac{(M_\nu - 1)}{\xi_{\nu,k}}} \cdot \tag{23}$$

Regardless of the channel quality or the QAM constellation employed, the layer-specific SNRs of all the activated MIMO layers are guaranteed to be equal in (23). Considering (10), (15) and (20), the BER for the ℓth MIMO layer at time slot k after the proposed PA strategy is obtained as

$$P_{\mathrm{BER}}^{(\ell,k)} = \frac{2\left(1 - \frac{1}{\sqrt{M_\ell}}\right)}{\log_2\left(M_\ell\right)} \operatorname{erfc}\left(\sqrt{\frac{3 \cdot p_{\ell,k} \cdot \xi_{\ell,k}}{4\,L\,(M_\ell - 1)} \frac{P_{\mathrm{s}}}{U_{\mathrm{R}}^2}}\right). \tag{24}$$

Taking into account (17) and (18), the average BER per MIMO data block P_{BER} after PA is calculated. So far the efficiency of adapting the transmit power level for fixed transmission modes is studied. However in order to achieve further enhancements in the BER performance, additional transmission parameters can be adapted to the varying channel state information, e.g., the modulation mode, the transmission rate, the coding schemes, the constellation size or any combination of these parameters [RR02, CG01]. At the cost of low signaling overhead, an adaptive Transmission Mode (TM) scheme is applied to minimize the overall BER. At each time slot, the proposed scheme selects one of the listed QAM constellations in Tab. 1 according to the lowest $P_{\mathrm{BER}}^{(k)}$. In this case a fixed data rate is guaranteed by selecting one of the predefined TMs minimizing the BER per time slot. Combining PA strategies with the adaptive TM scheme, significant improvements in BER performance are achieved.

5 Results

In this contribution the efficiency of the TMs listed in Tab. 1 for broadband (4×4) MIMO systems with 2 and 5 channel paths is investigated. Fixed data throughput of 8 bit/s/Hz is guaranteed when the predefined TMs introduced in Tab. 1 are employed. Furthermore, the efficiency of PA is studied. The BER curves for the investigated TMs are obtained by computer simulation and depicted in Fig. 1 and Fig. 2. From the simulation results, it can be seen that it is not necessary to activate all MIMO layers in order to minimize the overall BER for a predefined data throughput, e.g., the TM resulting in the best performance at a BER of 10^{-4} is $(16, 4, 4, 0)$ QAM as depicted in Fig 2. Further enhancements to

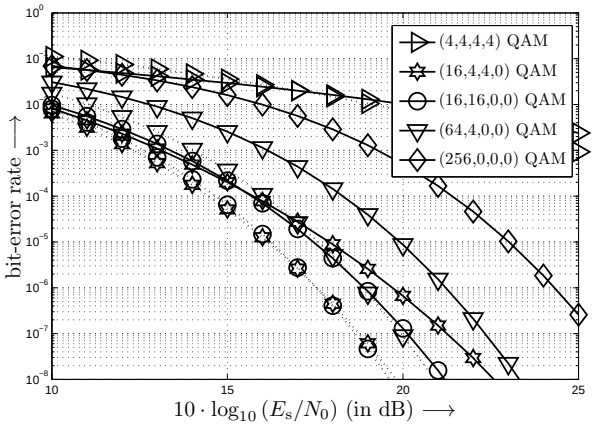


Figure 1: BER with equal-SNR PA (dotted line) and without PA (solid line) when using the TMs listed in Tab. 1 and transmitting 8 bit/s/Hz over frequency selective channels with $L_{\mathrm{c}} = 1$.

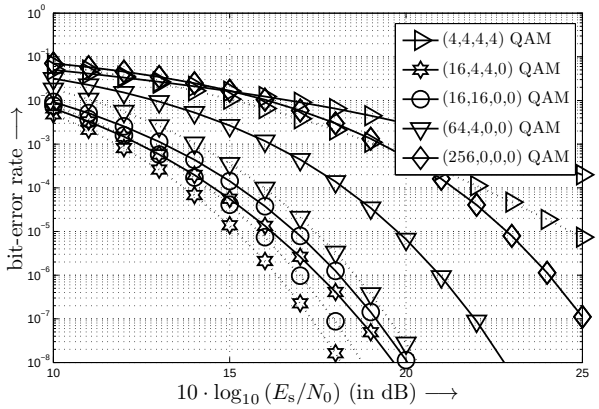


Figure 2: BER with equal-SNR PA (dotted line) and without PA (solid line) when using the TMs listed in Tab. 1 and transmitting 8 bit/s/Hz over frequency selective channels with $L_{\mathrm{c}} = 4$.

BER performance are observed by implementing adaptive allocation of transmit power. Additionally, upon analyzing the simulation results, the best TMs at a BER of 10^{-4} are specified and shown in bold in Tab. 1.

The performance of adaptive TM scheme is investigated. Allowing low signaling overhead, the BER performance of fixed TM scheme can be improved. An adaptive scheme selects the TM which minimizes the BER at each time slot instead of using fixed TM regardless of the channel quality. As depicted in Fig. 3, the adaptive TM scheme outperforms the fixed scheme. Furthermore, the efficiency of transmitting the QAM constellations shown in bold in Tab. 1 over frequency non-selective channel is studied in comparison with the investigated frequency selective 5-paths channel. As depicted in Fig. 4, it is observed that the BER performance of fixed TMs over frequency selective channels

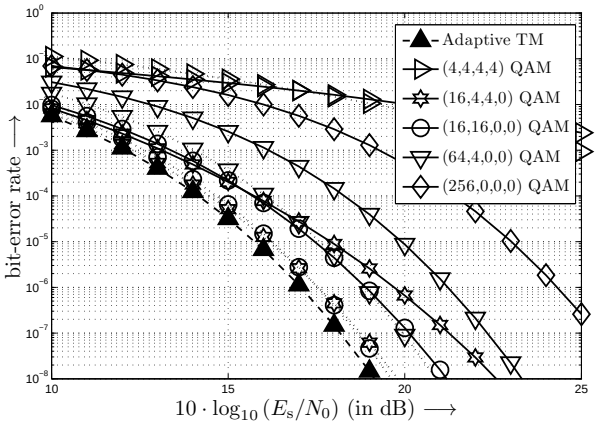


Figure 3: BER with equal-SNR PA (dotted line) and without PA (solid line) as well as adaptive choice of the TM combined with equal-SNR PA (dashed line) when using the TMs listed in Tab. 1 and transmitting 8 bit/s/Hz over frequency selective channels with $L_c = 1$.

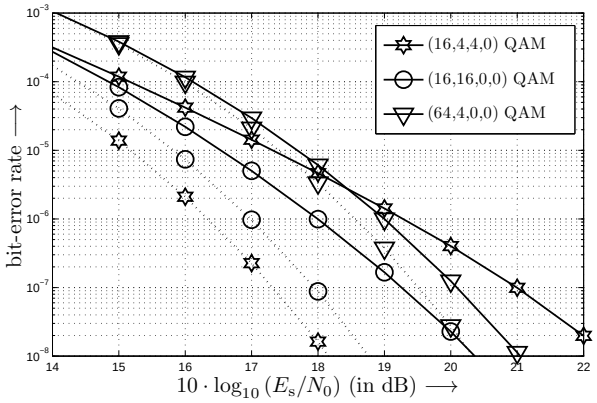


Figure 4: BER with equal-SNR PA when using the TMs shown in bold in Tab. 1 and transmitting 8 bit/s/Hz over frequency selective channels with $L_c = 4$ (dotted line) as well as frequency non-selective channels (solid line).

is more favorable. Therefore, multipath propagation is not a limiting factor in broadband MIMO systems.

6 Conclusions

Bit auctioning and power assignment strategies in SVD-equalized broadband (4×4) MIMO systems are investigated in this contribution. It turned out that the system BER perfor-

mance is substantially affected by the additional degrees of freedom introduced by the adaptive bit and power loading schemes. Additionally, in order to minimize the overall BER, activating all the MIMO layers is not necessarily required. Furthermore, the BER performance of the proposed bit and power loading schemes over frequency non-selective MIMO systems is studied in comparison to broadband MIMO systems. It is found out that for a fixed data throughput, the BER performance over broadband MIMO channels is more encouraging. Thus, the delay-spread of the broadband MIMO channel is beneficial in enhancing MIMO BER performance.

Acknowledgements

The authors wish to acknowledge the DAAD (Deutscher Akademischer Austauschdienst) for supporting the work developed in this investigation.

References

[AABP10] S. Aust, A. Ahrens, and C. Benavente-Peces. Modulation-Mode and Power-Assignment for SVD-and GMD-Assisted Downlink MIMO Systems. In *International Conference on Signals and Electronic System (ICSES)*, 2010.

[ABP09] A. Ahrens and C. Benavente-Peces. Modulation-Mode and Power Assignment in Broadband MIMO Systems. *Facta Universitatis (Series Electronics and Energetics)*, 22:313–327, December 2009.

[AG99] Mohamed-Slim Alouini and Andrea J. Goldsmith. Capacity of Rayleigh Fading Channels Under Different Adaptive Transmission and Diversity-Combining Techniques. *IEEE Transactions on Vehicular Technology*, 48:1165–1181, July 1999.

[AL08] A. Ahrens and C. Lange. Modulation-Mode and Power Assignment in SVD-equalized MIMO Systems. *Facta Universitatis (Series Electronics and Energetics)*, 21(2):167–181, August 2008.

[BZBO13] E. Bjornson, P. Zetterberg, M. Bengtsson, and B. Ottersten. Capacity Limits and Multiplexing Gains of MIMO Channels with Transceiver Impairments. *IEEE Communications Letters*, 17:91–94, January 2013.

[CG01] Seong Taek Chung and Andrea J. Goldsmith. Degrees of Freedom in Adaptive Modulation: A Unified View. *IEEE Transactions on Communications*, 49:1561–1571, August 2001.

[GD05] R. Gowrishankar and M.F. Demirkol. Adaptive M-QAM Modulation for MIMO Systems. In *IEEE/ACES International Conference on Wireless Communications and Applied Computational Electromagnetics*, Honolulu, Hawaii, April 2005.

[LXG02] Zhiqiang Liu, Yan Xin, and G.B. Giannakis. Space-Time-Frequency Coded OFDM Over Frequency-Selective Fading Channels. *IEEE Transactions on Signal Processing*, 50:2465–2476, November 2002.

[PL04] Chang Soon Park and Kwang Bok Lee. Transmit Power Allocation for BER Performance Improvement in Multicarrier Systems. *IEEE Transactions on Communications*, 52:1658–1663, October 2004.

[RR02] June Chul Roh and B.D. Rao. Adaptive Modulation for Multiple Antenna Channels. In *Conference Record of the Thirty-Sixth Asilomar Conference on Signals, Systems and Computers*, California, USA, November 2002.

[VPL10] P. P. Vaidyanathan, See-May Phoong, and Yuan-Pei Lin. *Signal Processing and Optimization for Transceiver Systems*. Cambridge University Press, April 2010.

[ZT03] Lizhong Zheng and David N. C. Tse. Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels. *IEEE Transactions on Information Theory*, 49:1073–1096, May 2003.

Optimal Detection in non-orthogonal CDMA-based Multiuser Transmission Schemes

Susanne Schumacher[1], Andreas Ahrens[1], César Benavente-Peces[2]

[1]Hochschule Wismar, University of Technology, Business and Design
Philipp-Müller-Straße 14, 23966 Wismar, Germany

[2]Universidad Politécnica de Madrid
E.T.S. de Ingeniería y Sistemas de Telecomunicación
Ctra. Valencia. km. 7, 28031 Madrid, Spain

email: andreas.ahrens@hs-wismar.de, cesar.benavente@upm.es

Abstract: Code division multiple access (CDMA)-based multiuser transmission schemes have attracted a lot of attention and enable the users to transmit their data at the same time and within the same frequency band. For user separation, orthogonal codes can be used. However, the orthogonality is lost in frequency-selective channels, and appropriate signal processing strategies have to be applied. Additionally, the received user-specific signal amplitudes can be significantly different which doesn't necessarily influence the quality of the signal detection as long as optimal detection is used as shown in this contribution. Our results show that in non-orthogonal transmission schemes the weak received signals can be detected with the same quality compared with strong ones when an optimal signal detection is used.

1 Introduction

The demand on transmission capacity for speech, data and multimedia information is expected to grow at least by a factor of five to ten in the next years. Unfortunately, the resources such as transmit power or bandwidth are limited. Within the last years, multiple-input multiple-output (MIMO) systems have attracted a lot of research activity since the channel capacity increases linearly with the minimum number of antennas at both the transmit and receive sides. Additionally, the use of adaptive modulation allows adapting to wireless channel changing conditions. On the other hand, the available resources have to be shared by the users. Two well-known channel access techniques are time division and frequency division multiple access which allow the users to transmit their data at different time slots and/or in different frequency bands, respectively. Given the users want to use the medium at the same time and within the same frequency band, code division multiple access (CDMA) based schemes seems to be a promising solution. Here the different users are separated by user specific signatures, where orthogonal codes are able to avoid any kind of interference in Gaussian channels. However, the interference immunity is lost if the channel becomes frequency-selective. In this situation, the Rake receiver could be an

appropriate solution. Additionally, when considering a multi-user CDMA based system, the received signal power could be significantly different, which is also known as the near-far problem. In such situations it might be difficult to detect the particular user's weak received signals unless a nearly optimal detector is used.

In this work it is shown that when using an optimal detection, the weak received signals can be detected in non-orthogonal channel situations at the same quality compared with the strong received signals.

The remaining part of the paper is structured as follow: Section 2 introduces the multiuser MIMO system model. The corresponding design of the optimal detector is presented in section 3. Simulation results are presented in Section 4 followed by the concluding remarks.

2 System model

In this work a two-user CDMA-based system model as shown in Fig. 1 is investigated. The user-specific data symbols $a_1[k] \in \{+1, -1\}$ and $a_2[k] \in \{+1, -1\}$ are multiplied

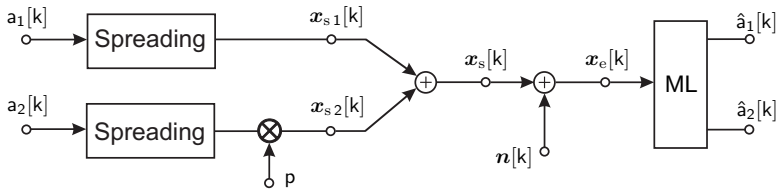


Figure 1: Two-user CDMA-based system

by their individual spreading codes $\boldsymbol{b}_1$ and $\boldsymbol{b}_2$ to form the user-specific transmit signals $\boldsymbol{x}_{\mathrm{s}\,1}[k]$ and $\boldsymbol{x}_{\mathrm{s}\,2}[k]$ at the kth symbol interval. Analytically, the transmit signals are given by

$$\boldsymbol{x}_{\mathrm{s}\,1}[k] = a_1[k] \cdot \boldsymbol{b}_1 \quad \text{and} \quad \boldsymbol{x}_{\mathrm{s}\,2}[k] = a_2[k] \cdot p \cdot \boldsymbol{b}_2 \ , \tag{1}$$

where p is the weighting factor describing the transmit amplitude difference between the users. The overall transmit data vector

$$\boldsymbol{x}_{\mathrm{s}}[k] = \boldsymbol{x}_{\mathrm{s}\,1}[k] + \boldsymbol{x}_{\mathrm{s}\,2}[k] \tag{2}$$

is transmitted and disturbed during the transmission by an additive, white Gaussian noise $\boldsymbol{n}[k]$ resulting in the received vector

$$\boldsymbol{x}_{\mathrm{e}}[k] = \boldsymbol{x}_{\mathrm{s}}[k] + \boldsymbol{n}[k] \ . \tag{3}$$

The task of the receiver is now to find the most likely transmitted data signals.

3 Receiver Design

By coding the transmit signals using orthogonal spreading codes, multiuser interferences can be avoided in AWGN channel conditions. However, in a non-orthogonal system multi-user interferences will appear and make it difficult to detect weak user-specific signals. However, having an optimal detector the user-specific signals can be detected with the same error-probability independently of their individual transmit powers. In order to implement an optimal detection, the received signal has to be compared with all possible transmit signals, which are composed of the actually viewed two-stages input alphabet as shown in Table 1. For finding the most probably transmit signal, the smallest distance be-

Table 1: Possible transmit signals assuming a two-stages input alphabet

μ	$a_1[k]$	$a_2[k]$	$\boldsymbol{x}_{\mathrm{s}}^{(\mu)}[k]$
1	$+1$	$+1$	$+\boldsymbol{b}_1 + p\,\boldsymbol{b}_2$
2	-1	$+1$	$-\boldsymbol{b}_1 + p\,\boldsymbol{b}_2$
3	$+1$	-1	$+\boldsymbol{b}_1 - p\,\boldsymbol{b}_2$
4	-1	-1	$-\boldsymbol{b}_1 - p\,\boldsymbol{b}_2$

tween the received signal vector $\boldsymbol{x}_{\mathrm{e}}[k]$ and the potential transmitted signal vectors $\boldsymbol{x}_{\mathrm{s}}^{(\mu)}[k]$ have to be found [For72, Ver98]. Analytically, the following metric has to be implemented

$$\min_{\forall\,\mu} \left|\left| \boldsymbol{x}_{\mathrm{e}}[k] - \boldsymbol{x}_{\mathrm{s}}^{(\mu)}[k] \right|\right|^2 \quad , \tag{4}$$

where $\boldsymbol{x}_{\mathrm{s}}^{(\mu)}[k]$ is given in Table 1. Once the most-likely transmitted signal has been determined, the corresponding user data signals are known as well. The appropriate operation of the optimal receiver assumes that the disturbance is a random variable (AWGN) added to the deterministic part of the received signal. Only the distance between potential transmitted signal vectors $\boldsymbol{x}_{\mathrm{s}}^{(\mu)}[k]$ influences the error performance of the data detection.

4 Results

In the following part the detection of the data signal of the first user $a_1[k]$ is analysed. As non-orthogonal spreading sequences are used, the second user acts as a disturbance, considered as a given multi-user interference. The results of the optimal detection are shown in Fig. 2 and Fig. 3 which represent the probability of error for the first user for different weighting factors p as a function of the bit energy of the first user $E_{b\,1}$ to the noise power spectral density N_0. The independent detection of the user signals produces, as known in the literature [EB01, FAJ03, DA01], an insufficient quality of the data detection.

The results obtained by the optimal detection show that the quality is almost independent

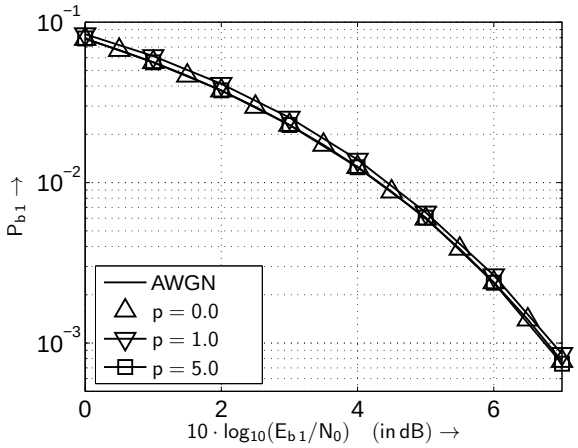


Figure 2: Bit-error-rate $P_{\mathrm{b}\,1}$ as a function of the signal- to- noise ratio $E_{b\,1}/N_0$ using optimal detection (spreading sequences $\boldsymbol{b}_1 = (+1,\, +1,\, +1)^{\mathrm{T}}$ and $\boldsymbol{b}_2 = (+1,\, -1,\, +1)^{\mathrm{T}}$)

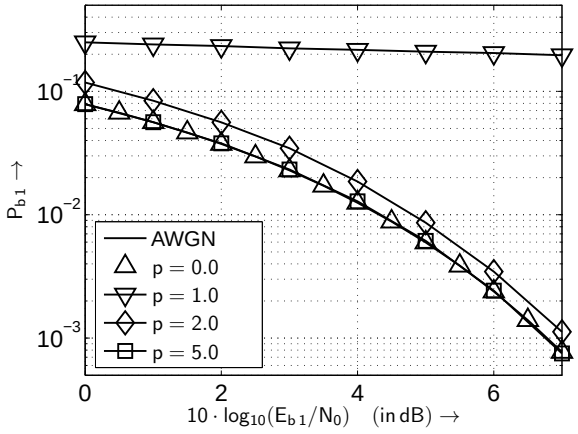


Figure 3: Bit-error-rate $P_{\mathrm{b}\,1}$ as a function of the signal-to-noise ratio $E_{b\,1}/N_0$ using optimal detection (spreading sequences $\boldsymbol{b}_1 = (+1,\, +1,\, +1)^{\mathrm{T}}$ and $\boldsymbol{b}_2 = (1+,\, +1.1,\, +0.89)^{\mathrm{T}}$)

of the intensity of the disturbing users (here the data signal of the second user), described by the weighting factor p. As shown in Fig. 3 the quality of the data detection is only influenced by the distance between the available overall transmit data vectors $\boldsymbol{x}_{\mathrm{s}}^{(\mu)}[k]$. Having disturber with nearly the same power compared to the user-signal to be detected, the error probability will increase (Fig. 3).

5 Conclusions

In this investigation a CDMA-based multiuser transmission in an AWGN channel has been analyzed considering the case in which orthogonality is lost due to the channel behaviour. In order to evaluate the proposed transmitter/receiver scheme some simulations have been performed for the case of two users in which the strength of the signal of one of the users arrives at the receiver more attenuated than the other one. The results have shown that the intensity of disturbers (known as multi-user interference) doesn't necessarily lead to a significant loss in the quality of the data detection as the performance is acceptable as shown in Fig. 2. However, the performance of the optimal detection is strongly affected by the distance between potential transmitted signal vectors. Having a small distance between the potential transmitted signal vectors and assuming that both users transmit with similar power the bit-error rate (BER) rises when using optimal detection (as shown in Fig. 3).

References

[DA01] P. Darwood and I. Alexander, P. amd Oppermann. LMMSE Chip Equalisation for 3GPP WCDMA Downlink Receivers with Channel Coding. In *International Conference on Communications (ICC)*, pages 1421–1425, Helsinki (Finnland), 11.–14. Juni 2001.

[EB01] H. Elders-Boll. Performance of an Adaptive LMMSE Chip Equalizer for UTRA-FDD Downlink Detection. In *Multiuser Detection in Spread Spectrum Communications (COST 262 Workshop)*, pages 1–6, Schloss Reisenburg nahe Ulm, 17.–18. Januar 2001.

[FAJ03] A. Feistel, A. Ahrens, and K. Jaeckel. Performance of a Correlation Receiver with a Feedback Equalizer in a CDMA Based Wireless Local Loop Environment. In *13th Virginia Tech Symposium on Wireless Personal Communications*, pages 115–122, Blacksburg (USA), 4.–6. Juni 2003.

[For72] G. D. Forney. Maximum-Likelihood Sequence Estimation of digital Sequences in the Presence of Intersymbol Interference. *IEEE Transactions on Information Theory*, 18(3):363–378, 1972.

[Ver98] S. Verdu. *Multiuser Detection.* Cambridge University Press, Cambridge, 1998.

Analysis of Social Network Success Factors for International Collaboration

Jan M. Pawlowski, Adewale A. Ademowo
University of Jyvaskyla, Finland
email: jan.pawlowski@jyu.fi, adewale@ademowo.me

Abstract: The terrain of social networking has changed the way we are connected as individuals and corporate bodies. The era of social networking has created lots of open opportunities to individuals and corporate bodies. There are successes and barriers therein. This paper identifies the success factors of social networking and collaborative websites to derive an analysis scheme. The derived scheme comprises of success factor themes and indicators with measuring approaches for social networks and collaborative websites. The identified social network success factors, success themes, indicators, and measuring approaches provide valuable insight into the behaviours and relationships that organisations must maintain to develop a successful social media presence, most especially for projects with international collaboration.

1 Introduction

The main aim of this paper is to assess the success factors of social networks applicable for international collaboration in order to develop an analysis scheme. The analysis scheme will be a valuable framework for measuring the successes of social networks in collaborative platforms. The increasing trends of social networking and their values have caused concerns for industries and academia. The terrain of social networking has changed the way we are connected as individuals and corporate bodies. The increasing popularity of social networks points to an evolution in the interaction between people and the society [WM08]. The era of social networking has created lots of open opportunities to individuals and corporate bodies. Social networks have several challenges covering the successes to overcome barriers.

This paper, while reviewing the concept of social networking in the previous and current research in the domain, considers the perceptions and feelings of the people towards social network successes. It also examines the various definitions, meanings, benefits, purposes, and entities / processes of social networks. The importance of social networks cannot be over-emphasised as the key findings of previous research collectively highlight them in the areas of communication, collaboration, networking, and sharing. These areas are vital to individuals and organisations who consider social networks as tools in the various activities. It is imperative to study both the successes and barriers of social network and social networking tools or sites before coming up with an acceptable analysis scheme. In this view, this paper examines both the success factors and barriers, and then identifies the success factors to overcome inherent barriers and that are applicable to the context of this

study. In achieving the above, this paper identifies the key themes of social network success factors from various viewpoints; harmonises the viewpoints and develop an analysis scheme which revolve around content, people, culture, technology and value; evaluates the scheme to ensure its alignment with social network scenario most especially in international collaboration, and the validate the scheme with empirical investigation of EU projects.

The paper tends to proffer solutions to three research statements, namely; i. How can social networks for international collaboration be assessed? ii. Has there been any analysis scheme with indicators to assess the success factor of such platform? iii. What is the applicability of the indicators to existing collaborating project websites? The research methodology being an exploratory case study utilises both qualitative and quantitative. [Yin03] defines case study research as "an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident." In support of the definition, [Woo10] explains that case study research focuses on describing, understanding, predicting, and/or controlling the individual (such as process, people, and organisation). Therefore, Woodside submits that an objective of a case study research may combine any of description, understanding, prediction, and control. In gathering the data; the researchers review previous literature in the field, administer questionnaires for the administrators of the selected EU project websites, and conduct observation and content analysis of the websites.

The assessment of the success factors of collaborating project websites and the previous studies on the success factors of social networks lead to the analysis scheme. The scheme developed is a theoretical framework that can apply to social media enabled websites and international collaborative platforms. The themes, indicators and measuring approaches can be adopted in and applied to international collaborative websites. The analysis scheme can provide valuable insight into the behaviours and relationships that organisations must maintain to develop a successful social media presence with the necessary attention to efficiency and effectiveness that will ensure greater productivity.

2 Background

Social networking has been in existence before the advent of the Internet or mass communication [WM08]. The Internet is the mainstream channel for information exchange and social interaction [RL09]. There are several definitions and descriptions found from the literature review that describe well enough what it means to network in social context, and the perfect meanings of a social network vis--vis social networking, social networking tools, social software, and social networking site.

The term social network or social networking is often inter-relatively used. [RM10] terms social networking as enabling people to collaborate, share ideas and engage around messages. Social networking tools are enablers of social networks such as web applications, websites, and other engines used in ensuring social interaction. A social networking site can be defined as Web 2.0 technology that enables collaboration and participa-

tion [CMR09]. It can be understood that social network depends on the people and their social interaction; the fact which [WM08] highlight by presenting social networking as the logical extension of human tendencies toward togetherness. In these views, social networking may be equated to people that tend to connect people with the purpose of enabling interaction among each other and sharing information within the social network or group.

A social networking site is an Internet-mediated and web-supported social interaction platform that tend to relate people's social inclination in a predefined group or circle called social network. A social-networking website allows users to post their personal information and create personal networks to exchange information with other users [WM08]; which [KH10] support in their definition of social networking websites as applications that allow users to connect each other by creating personal information profiles, inviting friends to access their profiles, and sending e-mails and instant messages between each other. [LVL03] also define social networking websites as online communities or cyberspaces supported by information and communication technologies, centred upon communication and interaction to generate content, and build a relationship.

Previously, people thought of the Internet as an information repository, the emergence of social networks is turning it into a mechanism for connecting people [WM08]. Social networking can be seen as a family or association through which social interaction occurs. The influence of social networking is inherent in its shared values achieved through people's interaction, collaboration, and communication; which implies that a team or group work is usually better than one-man work. Ability to work together in groups, creating distinctive value, is one of the greatest assets [WM08].

2.1 Benefits and Purpose of Social Networks

The concept of social networking is a part of the social media, which use mobile and web-based technologies to create highly interactive platforms via which individuals and communities share, create, discuss, and modify user-generated content [KHMS11]. [RL09] identify several benefits of online communities as social networks for individuals and organisations. The benefits are factors instigated by the purposes of social networks to the users. The identified benefits focus on information exchange, social support, social interaction, time and location flexibility, and permanency for individuals; and collaboration, customer loyalty, employee communication and trust, visibility and reputation, and productivity for organisations.

[KHMS11] developed a framework in the figure 1 below which compares and contrasts the functionalities and the implications of different social media activities as inherent in their purpose. The framework informs the need for social networks.

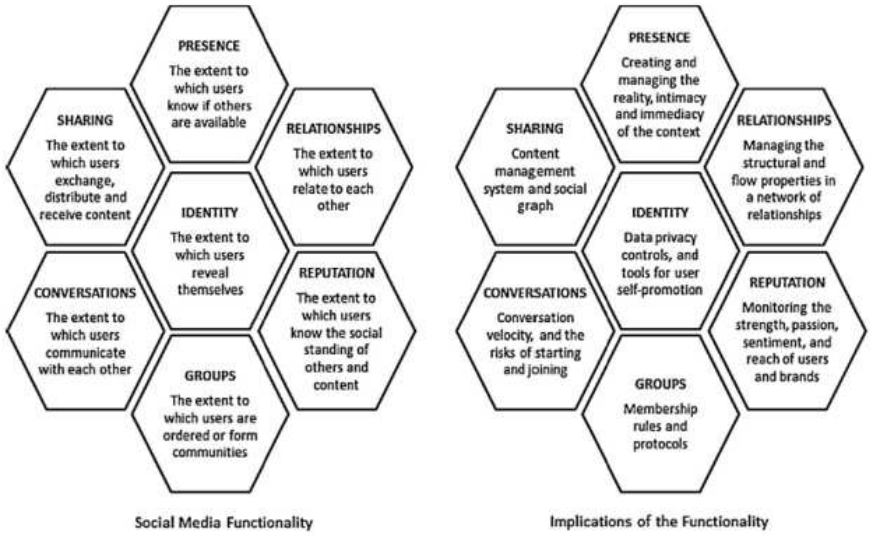


Figure 1: The honeycomb of social media [KHMS11] (p243).

The framework identifies seven functionalities of social media, which include conversations, groups, identity, presence, relationships, reputation, and sharing. They facilitate examination of facet of social media user experience and its implications for organisations. These functionalities are further streamlined to form the social network entities or processes which the next chapter expatiates.

2.2 Social Network Entities / Processes

Social entities are categories of processes performed by social networks. The entities are collective names that classify social network according to their functions and features. According to [WM08], the four key processes are communication, collaboration, networking, and sharing. Collaboration is an aspect that concerns this paper. It facilitates the analysis through the successes of social networks and their importance to international collaboration. The following list briefly explains the processes while analysing the successes of social networks in international collaboration:

- **Communication**: Social network in this context means passing information from one person to another or from one end to another. People engage in social networking for the purpose of sending messages to each other.
- **Collaboration**: Social network in this context means people use social networking tool / site to carry out tasks with common goals and objectives. In social collaboration, development projects may be carried out in a socially-networked environment and among globally distributed team or groups.
- **Networking**: Social networking makes meeting between people convenient. It

makes socialising seamless because people can be connected and reached easily. Social networking implies individuals using the Internet to communicate in unimaginable ways [WM08].

- **Sharing**: Social sharing entails utilising social software or tools on sharing information, files and documents.

Communication, collaboration, networking and information sharing have been the core values of social network, which makes it more endearing to individuals and organisations. Social networking helps people maintain contacts, communicate and exchange information with each other [YLL+09]. The processes of social networks entail communication, collaboration, networking and sharing while the purpose involves utilisation by people in satisfying their needs in the identified processes.

2.3 Success Factors of Social Networks

The growing trends in the adoption and use of social networks like social networking sites like Facebook, Twitter, and Myspace; social software; and social networking tools are entrenched in various factors. These factors revolve around people, technology, culture, and obtainable value. The effective utilisation of these factors results in social network success. A series of research elucidates the success stories of social networks and related entities. Previous literature reveals lots of success factors [M.10, Bel09, CMR09, DL86, IMP09, KH10, Man10, Mar05, RL09, RM10, SWC76, WM08, YLL+09] but this paper only consider those closely related to the context of collaboration in international projects.

In assessing the success of a social network, success should not be seen as similar to profit but considers both the profit and the value that ensures users' rewards from their interests. In addition to the users' interests, the assessment also considers the overall worth of the platform measured with users in mind, the importance of value proposition, and cost. Users interests may be time, money, or energy investment. Users satisfaction plays a pivotal role in the success of a social network [M.10]. The satisfaction depends on what users derive from the adoption and use of the platform. [WM08] while analysing MySpace /Friendster, Facebook, Wikipedia and YouTube confirmed the users' impacts on social network success; and effects of tools for easy expression and user interaction, and flexibility and responsiveness which characterise the successes of MySpace and Friendster. Weaver and Morrison further state that Facebook's extensive tools, documentation, and an application programming interface (API) for third-party developers to use in creating "applications" gives it headway above other social networking sites. [YLL+09] also agree that compelling user interfaces, tools for importing and exporting data, and ease of setting up the social application / software are success indicators for social networks.

[KH10] while referencing [SWC76] identify the social presence as a key factor. The three defining social presence as the acoustic, visual, and physical contact that can be achieved; further state that high social presence results to a broad social influence that the communication partners have on each other's actions. Daft and Lengel (1986) also

identify media richness as a factor and it depends on the assumption that the goal of any communication is the resolution of ambiguity and the reduction of uncertainty.

Implementing privacy settings based on users' feedback [WM08] is a factor to reckon with as mostly, privacy issues have been ravaging social network success. Consideration for Five B's of [KH10] which is be active, be interesting, be humble, be unprofessional, and be honest can fashion goodwill for a social network success. [WM08] identify OpenSocial as a platform that will enhance the future success of social network because it will create an avenue for developers to create a single application that seamlessly spread across all social platforms. OpenSocial is Googles open source framework which is still in planning/incubation stage.

[RM10] confirms that social networking in business is becoming a significant force for communication and collaboration in todays business world and supports his claim with Gartner's prediction. [Gar10] predicts that the availability of social networking services combined with dynamic demographics and work ethics will influence 20 percent of users to make social networks their business communication hubs. In order to meet up the challenges, organisations must be collaboration-ready and provide tools that enhance sociability and usability in the organisations' processes. Technology does not work but effective use of technology makes things work. The overall success of social networks depends on people.

In summary, the success factors of social networks revolve around content richness, timely engagement, platform users, social presence, culture and consideration for multilingualism, usability and navigability, and platform mobility. Tools that enhance expression, interaction, integration, flexibility and responsiveness, and documentation also matter. In addition to the pools of success factors are data privacy and integrity, platform setup features, feedback systems, data management features, value proposition to the users, and the benefits to the platform owners.

2.4 Barriers of Social Networks

For all successful scenarios, there must be some traces of shortcoming. In any analysis that relays success factor, the conflicting barrier must be examined. Adequate control of risks poses by barrier leads to success itself. In this view, the researchers review and consider social network barriers in the analysis. The recent rise in popularity of online social network applications raises serious concerns about the users' security and privacy [CMS09]. [WM08] corroborate this by identifying privacy issues as parts of the core barriers, and data reliability and bias, susceptibility to vandalism, and pornography or offensive content in the cases of MySpace, Facebook, Wikipedia and YouTube.

[YLL+09] while making their submissions also agreed with privacy issues. They further raise concerns over information silos, which make information on a website not working with the others. In consideration for security concern, there is a need to consider factors like information control and ownership, and information accountability. The existing social networking services maintain the centrality while the organisations behind the services

maintain control and exclusive authority over all the data of the users.

Content communities bear the risk for the sharing of copyright-protected materials [KH10]. [CMS09] in their views identify six barrier concerns of social networks as an end-to-end confidentiality, privacy, access control, data integrity, authentication, and availability; which tally with the views of the other researchers previously cited. Self-preservation of identity is one of the problems affecting the structure and underlay principles of social networking services [Mar05].

In summary, the success factors of social networks should be able to overcome the identified barriers and risks like users' security and privacy, data privacy and integrity, offensive contents, information control and ownership (intellectual property), and copyright-protected content.

3 Analysis

This chapter focus on the derivation of analysis scheme that serves as a framework for assessing the success of a social network for international collaboration. This study considers the social network success factors and identifies the key theme that relates and harmonises various viewpoints to arrive at a confluence. The analysis scheme is structured with themes, components, and the supporting sources. The themes being the primary determinants anchored by the components reflect on the main points of consideration to assess the successes of a social network for international collaboration as the Table 1 describes. The analysis scheme constitutes the factors that are influential to the successes of social networks. The focus of this analysis scheme is to streamline and establish a framework for evaluating the success factors of social networks that are relevant to international collaboration. This leads to the derivation of social network success analysis scheme as informed by the identified themes with their corresponding components which Table 1 below represents:

Table 1: Social Network Success Analysis Scheme (SNSAS)

Theme	Components	Sources
Content	Content / Media richness; Timely engagement; Content Control and Ownership.	Banbersta, 2010; Belniak, 2009; Daft & Lengel, 1986; Ribera & Leroy, 2009; Kaplan & Haenlein, 2010; Manikandan, 2010
People	User population; Social presence / Sociability; Being active, interesting, humble, unprofessional and honest.	Ribera & Leroy, 2009; Kaplan & Haenlein, 2010; Marwick, 2005; Short et al., 1976; Weaver & Morrison, 2008
Culture	Recognition of Cultural differences; Consideration for multilingualism.	Roberts, 2010
Technology	Tools for easy expression and user interaction; Easy to integrate; Extensive tools and documentation; Application Programming Interface (API); Usability / Good user interfaces; Tools for importing and exporting data; Ease of setting up the social application / software; Flexibility and responsiveness; Privacy settings based on users' feedback; Mobile application / Go mobile.	Banbersta, 2010; Belniak, 2009; Chui et al., 2009; Isaas et al., 2009; Kaplan & Haenlein, 2010; Manikandan, 2010; Roberts, 2010; Weaver & Morrison, 2008; Yeung et al., 2009
Value	User benefits; Return from time, money, or energy investment; Simplicity, focus, and openness; Overall worth (prize) of the platform.	Banbersta, 2010; Isaas et al., 2009; Roberts, 2010

Content, People, Culture, Technology, and Value are five themes of success analysis scheme and serve as the core tenets of the scheme. The core tenets originate from the wider perspectives of the success factors of social networks. They serve the main motive of deriving harmonised and acceptable themes with indicators for empirical analysis of social network success factors. The scheme above motivates the social network success indicators with their measurement approaches, which Table 2 below highlights.

Table 2: Social Network Success Indicator (SNSi)

Theme	Indicators	Measurement Approach
Content	Quality of content / Quality Assurance; Number of content shared daily (Quantity); Content page view per da.	Survey of the users; System features and log statistics; System features and log statistics.
People	Number of users; Number active users; Frequency of Participation / Interaction.	System features and log statistics
Culture	Number of Languages; Number of Nationalities	System features and log statistics
Technology	Is the platform cross-browser enabled? How many browsers are supported? Is the platform mobile-enabled? What mobile platforms are supported? Types of tools integrated; Level of accessibility; Level of usability (UI); Speed of responsiveness; Level of privacy settings based on feedback.	System features and log statistics; Interviews with technicians and administrators; Survey of the users.
Value	Ratio of contribution; Ratio of the issues raised to issues resolved; Return over Investment (RoI).	Survey of the users; System features and log statistics; Platform overall productivity; Platform financial worth.

The social network indicator evaluates each of the themes with their corresponding indicators following the recommended measurement approaches. Meanwhile, it has to be noted that not all aspects can be represented by indicators. Therefore, the researchers focus on measurable factors only. The indicators consider the components highlighted in Table 1 and measure each theme based on their components. Subsequent to the application of the indicators, the researchers consider certain measuring steps which affect the organisational objectives, types of measurements, measurement levels, and measurement tools, which [IBM10] recommends. The researchers also improve the measuring technique used in Wiki Success Model [RSU+09].

The scheme presents the main themes which are content, people, culture, technology and value. It clearly indicates what needs to be measured by the indicators while the measurement approaches defines the method to adopt in confirming the essence of the indicators. The analysis scheme focuses on social network use in international collaboration.

4 Discussion

In setting indicators for measuring the success factors of social networks; content, people, culture, technology, and value are the key themes to recognise. The researchers identify the indicators with their corresponding measurement approaches for each category to serve as benchmarks for their application in practice. The indicators contain elements that describe the main activities performed on social networks and the significance of their impacts. This paper adapts measurement approaches in order to assess the impacts of the indicators.

[IBM10] reiterates the importance of establishing a measured approach and concludes that it captures information about the usage of social software tools; how social networks influence individual, group and organizational behaviour; and the business value derived from the investment in social software technology. Hence, the measurement approach helps identify the success of social networks and the level of Return over Investment. The researchers note that measuring the success of a social network depends on the need of the organisation as inherent in its objectives to the use of social networking.

The derived social network success scheme and indicator provide useful insight into the behaviours and relationships that organisations must maintain to develop a successful social media presence and enhance effective collaboration.

This study utilises both qualitative and quantitative methods. The indicators such as content quality, platform compatibility, tools, accessibility and usability, privacy, and issue resolution are qualitatively measured. While the indicators like content sharing, page views, user base, participation rate, languages, nationalities, speed of response, and Return over Investment (RoI) are quantitatively measured.

4.1 Empirical Investigation of EU Projects

The empirical part of this study comprises questionnaire administration, observation, and content analysis. The empirical studies focus on the selected EU project websites to test the derived analysis scheme. The questionnaire examines the core themes of the analysis scheme identified in Table 2 which includes content, people, culture, technology, and value. Table 3 below briefly highlights the basic statistics of email sent (questionnaires administered), delivery failure, email acknowledgement and the responses:

Table 3: Basic Statistics of Questionnaire Administration

Item	Number
Identified EU Projects	30
EU Project websites with contact email / web form	27
Email Delivery Failure	2
Email Acknowledged	7
Questionnaire Responded	4

As indicated in Table 3 above, only four responses came from the 27 questionnaires dis-

patched. Due to the low response rate, the researchers use observation and content analysis methods to further test and validate the analysis scheme with the aid of third-party tools. Project websites hosted on sub domains are not considered because of the parameters applied in implementing the analysis measures. To test and validate the themes in the analysis scheme, the researchers use third-party online tools such as Alexa Ranking, Google Page Rank (PR), Mustat, Site Cost Calculator, WooRank, Worth of Web, Yandalo, and YSlow.

The successive sub-chapters discuss the outcome of the questionnaires, observation and content analysis with the consideration of the success analysis scheme in tandem with content, people, culture, technology, and value; and their relationships with social network for international collaboration. The outcome of the empirical part emanates from the qualitative and quantitative analysis of the available data.

4.1.1 Content

Content richness is an important factor in determining the success of a social network for international collaboration because it is the first point of attraction to the users. It defines the essence of the platforms existence. According to the respondents, no quality measures or assurance considered apart from the level of checks by some of the project coordinators. They are aware of the number of contents published periodically but have no records of the content performance and utilisation outside the project team.

From the observation and content analysis perspective, the researchers consider three key factors that determine the quality of a website. They are media richness, timely engagement, and usability. In order to have a benchmark for the websites, the researchers use Google Page Rank and Alexa parameters for the content analysis with respect to the content relevance in regional and global views; and the traffics. The Figure 2 below showcases the Page Rank and Alexa parameters for the websites:

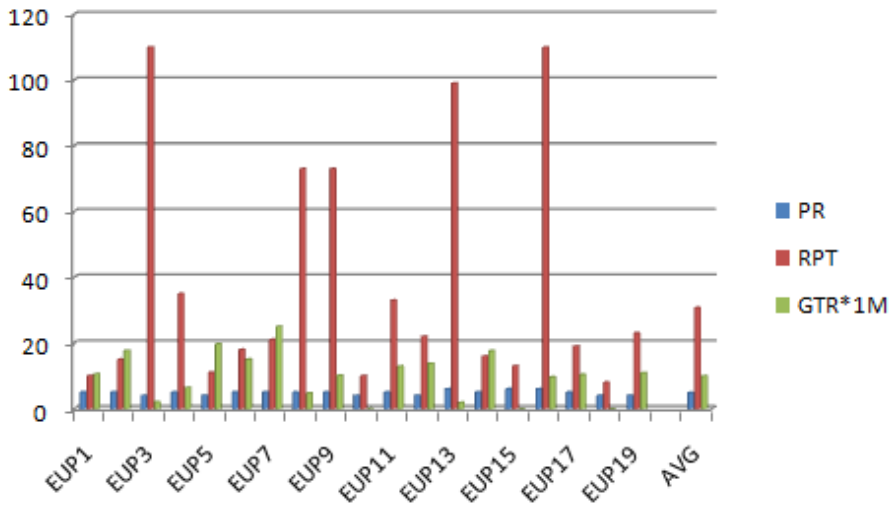


Figure 2: Content PageRank and Alexa Traffic Ranking

In the figure above, the following acronyms are used:

- Page Rank = PR (score over 10)
- Reputation (Content Relevance to other websites) = RPT
- Three-month Global Alexa Traffic Ranking = GTR

The average page rank (PR) is 4.84 / 10 which serves as a benchmark for the websites. The websites are quite good with their page ranks ranging from 4 to 6 according to Google. The page rank indicates their search relevance in the global scale. Alexa reputation (RPT) indicates the websites relevance to other websites or users from other websites. It indicates a series of back links to the project websites. As for the websites, none of them show any relevance in their respective countries according to Alexa county traffic ranking (CTR) because no data were available for them. Although, the websites ranked globally, but their average indication is extremely low. The Alexa ranking operates such that rank 1 is better than rank 2. In this case average GTR is 9.91M. The measuring of success factor of the websites based on content and consideration for the benchmark above can be deduced with the following:

- The higher the page rank the better the website contents and more successful it is. The websites with page rank greater than 4.84 are more successful while those with lower page ranks are less successful.
- The higher the reputation, the more relevance the contents are. Websites with RPT higher than the average (30.74) are more relevant than those with RPT lower than the average. Although, a project may be relevant to a smaller community, i.e. it might be visited less but still has a higher value to the community. Therefore, the indicator serves as a first yardstick of how successful the site is. In that case, further information like users survey, system features and log statistics must be taken into account.
- The fact that the projects are EU-based, website visibility and relevance, assumed to be in the EU states. The websites with Alexa-mapped country (AC) in the EU states are more visible in their domain region than those outside EU states such as the website with their mapped countries in India, Indonesia, and Malaysia. The websites do not perform well in their region because their CTRs indicate no data.
- Nonetheless, the global traffic cannot be concluded upon, but the average among the websites can serve as a yardstick for measuring their success. The lower the Alexa traffic ranking, the higher the relevance of the ranked website in term of traffic from the users. Therefore, the websites with GTR lower than the average are more successful than the website with GTR greater than the average.

4.1.2 People

People are the drivers of technology and controllers of social networks. The role of people in the success of social networks are essential as all other themes of the identified success

factor analysis scheme depend on people. Some people create social network platforms for another sets of people to use. This implies that social networks are people-oriented, controlled by people and developed for people. Under this theme, the respondents do not consider users outside their circles. They limit the number of users to the project members. Appointed project members contribute to their websites.

People make technology work. The existence of a website is to meet people's needs. The number of people visiting a website determines the success of the website. Therefore, the researchers use numbers of visitors and page views as a benchmark to measure the successes of the websites through people. MuStat.com, a third-party analytics tool, is used to determine the Daily Visitors (DV) and Daily Pageviews (DP) statistics while the researchers consider the Social Presence (SP) by observing the websites for links to their social networking sites. The Figure 3 below summarises the findings in that respect:

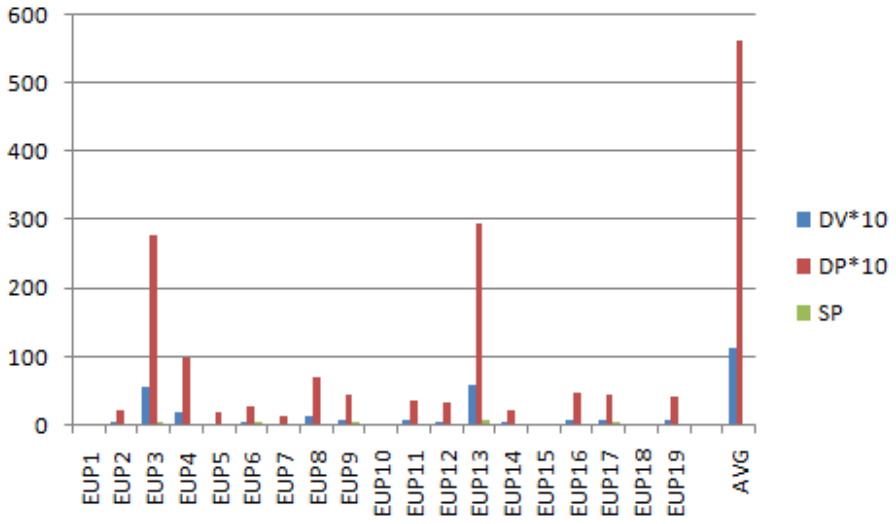


Figure 3: Websites Daily Visitors and Pageviews with their Social Presence.

Considering the people factor analysed with websites visits and page views as the figure above indicates, the average values calculated to serve as benchmarks for this section apply. The websites with daily visitors and page views higher than the respective average are more successful than those below the benchmarked averages. Social presence is a factor that makes an impact if adequately utilised. The social presence behaviours from the figure above do not indicate efficient and effective use of social media by the organisation even though some of them registered their presence. Nine projects utilise at least 2 or at most 8 social networking websites including RSS. The use social networking sites like Facebook, Flickr, Google Group, Linkedln, SlideShare, SourceForge, TELEurope, Twitter, and YouTube. In addition, EUP16 has own internal social network which is active in its own capacity. Nonetheless, the future research within this study should consider the internal social networking functions.

4.1.3 Culture

Culture as the peoples way of life determine the success of a social network. It reflects on peoples language, religion, nationalities, and habits. In the context of this study, the only considerable cultural factors are language and nationalities. The websites of the respondents are in English language except for one which has two languages (English and Italian). In most cases, they know the number of nationalities participating on the websites.

People living where English is not their official or first language will be more attracted to websites with localisation than only English. To confirm the website's languages, the researchers observe the website. The websites use English language only except for EUP18 who has Italian as an additional language. Other factors identified can be examined with further empirical facts from the project administrators.

4.1.4 Technology

Technology is an enabler of social network functionalities. It entails the use of tools to ensure efficiency and effectiveness of a social network platform. It is indeed a reasonable success factor which people adapt in social networks. The websites of the respondents are cross-browser compatible. Content analysis reveals that all the project websites are cross-browser compatible because they render well on main web browsers like Chrome, Firefox, IE, Opera, and Safari . The project websites are mobile-friendly but do not have mobile apps or mobile version. Some of the websites use external applications / tools like SharePoint, Drupal, Wiki, and file repository for collaboration and content management. The project websites' administrators do not consider extra effort on the websites' accessibility and usability but depend on the website templates. They do not measure the speed of responsiveness but control privacy settings through the use of password for restricted areas where applicable.

Most of the components for determining the success factors of social networks exist in technology. Technology plays extremely crucial roles in various aspects as indicated in Table 1. Obviously, all the parameters cannot be tested without access to log files, but some parameters can be tested using the identified third-party tools like WooRank (WR) and YSlow (YS).

WooRank provides an overview of the key factors that influence the SEO and usability of a website. The rank is a grade, on a 100 point scale that represents the Internet marketing effectiveness. The algorithm depends on 50 criteria, which include search engine data, website structure, site performance etc. A rank lower than 40 implies that lots of areas need to be improved. Rank above 70 is a substantial mark, and it means that the website is probably well optimized (WooRank, 2012). WooRank analysis considers factors such as visitors, social monitoring, mobile, SEO Basics, SEO Content, SEO Links, SEO Keywords, SEO Authority, SEO back links, usability, security, and technologies.

YSlow analyses web pages and why they are slow based on Yahoos rules for high performance websites. It gives a score based on the performance of the page and offers suggestions for improving the pages performance [YSl12]. Both the WooRank and YSlow

measure the indicators identify under the technology theme element and their ratings for the overall performance of the websites which Figure 4 indicates below:

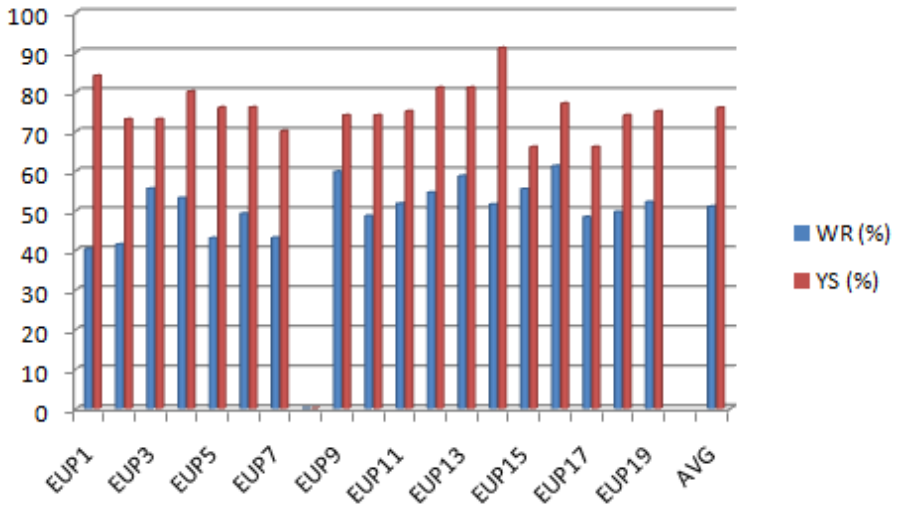


Figure 4: Technology Performance Measurement with WooRank and YSlow

The figure above shows the performance grades for the websites according to WooRank and YSlow. They form a benchmark for measuring the success factor of a social network considering the technology utilisation and adaptation; and the level of compliance with international standards. Accordingly to WooRank, 10 websites manage to have 50 percent while 8 websites fall below 50 percent. The WooRank analysis indicates that the websites are not so successful because of their performance grades. The performance grades fall below 60 percent except for EUP16 which has 61.2 percent. On the side of YSlow, the indicator favours the websites because almost all the websites have more than 70 percent except for EUP15 and EUP17 that have 66 percent performance grades.

4.1.5 Value

Value is another theme element that measures the impact of the value propositions to the end users, Return over Investment (RoI) to the owners, and the current worth of social network platforms. The respondents do not consider the valuation of their platforms because they do not take any measure to determine how well their websites are, and contents are faring to the visitors. They do not measure the successes of their websites because the projects are not profit-oriented.

The researchers use third-party web application tools like MuStat (MS), SiteCostCalculator (SCC), Yandalo (YD), and Worth of Web (WoW) to measure the current net worth value of the websites based on the theme indicators. The Figure 5 below shows the results of different website valuation tools used and the average net worth value of the websites.

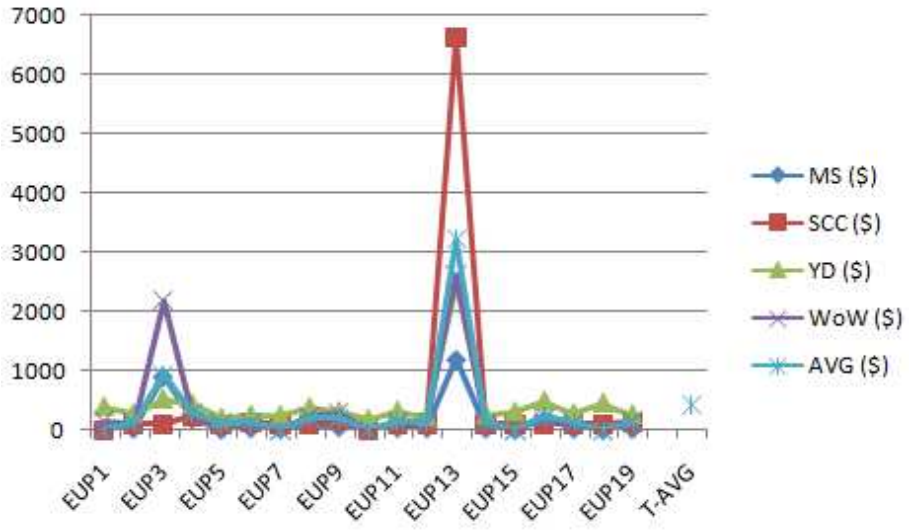


Figure 5: Net Worth Value of the selected Project Websites

The valuation outcomes in the figure above create benchmarks for analysis in the context of social network success factor measurement with respect to the value of the platform. The price does not include a certain situation on the IT market, as well as brand value or possible value of the company behind the site [Cal12]. The worth of the websites depends on public statistics covering daily visitors, page views, domain age, search engine inclusions, URL marketability, and loading time. The researchers consider different platforms to check the websites' worth because of the variance that occurs and the use of different parameters to calculate the website worth.

4.2 Relevance of the findings to Previous Research

The findings in this paper are relevant to the previous research and resourceful for future research. The analysis scheme derived with five main categories such as content, people, culture, technology, and value were independently considered in the previous research as factors affecting the success of social networks as highlighted in the Table 1.

The research involves deriving a unified framework by exploring previous literature to determine missing gap and utilising selected project websites for empirical fact findings. It complements existing studies in the field, formulates a new framework that can be used to assess the success factors of social networks for international collaboration.

5 Conclusions

Based on the literature, empirical study, observation and content analysis, and experience with social networks; the researchers propose an analysis scheme for measuring the success factors of social networks for international collaborations. The scheme is a theoretical and literature-based framework which comprises the themes and indicators with measurement approaches for determining the successes of social networks.

In the development of the scheme, the researchers find that several success factors of social networks exist non-unanimously from the previous research perspectives. Then, the researchers attempt to find a confluence of the success factors by deducing five theme elements (content, people, culture, technology and value) revolving around the success factors. The themes form the basis of the analysis scheme. The researchers empirically investigate the scheme with EU projects and find that the themes in the analysis scheme are relevant to measuring and analysing the success factors of social networks for international collaboration. Although, further empirical validation will improve the scheme.

The analysis scheme paves the way for further investigations in the research areas that measure the success factors of social networks. This paper only considers 27 EU projects with limited empirical investigation combined with observation and content analysis using third-party web analytic tools. The outcomes are the foundation for future empirical work in this area. However, the scheme needs further empirical validation to ascertain its applicability and generalisability.

References

[Bel09] A. Belniak. What Are the Critical Success Factors of A Social Network? Ill Tell You Over a Beer (advocate.com) @ONLINE., December 2009.

[Cal12] Site Cost Calculator. Estimate website cost and Calculate traffic @ONLINE., November 2012.

[CMR09] M. Chui, A. Miller, and R.P. Roberts. Six ways to make Web 2.0 work. *Business Technology - McKinsey Quarterly*, February 2009.

[CMS09] L.A. Cutillo, R. Molva, and T. Strufe. Privacy preserving social networking through decentralization. *IEEE Sixth International Conference on Wireless On-Demand Network Systems and Services*, pages 145–152, February 2009.

[DL86] R.L. Daft and R.H. Lengel. Organizational information requirements, media richness, and structural design. *Management Science*, 32(5):554571, May 1986.

[Gar10] Gartner. Gartner Reveals Five Social Software Predictions for 2010 and Beyond @ONLINE., February 2010.

[IBM10] IBM. White Paper - Measuring the value of social software (Defining a measurement approach that maps activity to business value) - IBM Software Services for Lotus June 2010. @ONLINE., June 2010.

[IMP09] P. Isaas, P. Miranda, and S. Pfano. Critical Success Factors for Web 2.0 A Reference Framework. 5621:354363, July 2009.

[KH10] M. Kaplan and M. Haenlein. Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53(1):5968, JanuaryFebruary 2010.

[KHMS11] J.H. Kietzmann, K. Hermkens, I.P. McCarthy, and B.S. Silvestre. Social media? Get serious! Understanding the functional building blocks of social media. *Business Horizons*, 54(3):241251, MayJune 2011.

[LVL03] F.S.L. Lee, D. Vogel, and M. Limayem. Virtual Community Informatics: A Review and Research Agenda. *Journal of Information Technology Theory and Application (JITTA)*, 5(1):4761, April 2003.

[M.10] Banbersta M. The success factors of the Social Network Sites Twitter@ONLINE., June 2010.

[Man10] K.S. Manikandan. Social Networking Critical Success Factors @ONLINE., February 2010.

[Mar05] A.E. Marwick. "I'm More Than Just a Friendster Profile: Identity, Authenticity, and Power in Social Networking Services.". *Association for Internet Researchers 6.0*, October 2005.

[RL09] A. Ribera and G. Leroy. A Life-Cycle Perspective on Online Community Success. *ACM Computing Surveys (CSUR)*, 41(2):1073–1096, February 2009.

[RM10] S. Roberts and M. Murray. White Paper: Critical Success Factors for Enterprise Social Networking - Four Tips for Ensuring the Success of Collaboration in Your Organization @ONLINE., 2010.

[RSU+09] P. Raeth, S. Smolnik, N. Urbach, , and C. Zimmer. Towards Assessing the Success of Social Software in Corporate Environments. In *Proceedings of the Fifteenth Americas Conference on Information Systems, San Francisco, California*, August 2009.

[SWC76] J. Short, E. Williams, and B. Christie. *The social psychology of telecommunications.* John Wiley and Sons, Ltd, Hoboken, NJ, 1976.

[WM08] A.C. Weaver and B.B. Morrison. Social Networking. *IEEE Computer*, 41(2):97–100, February 2008.

[Woo10] A. Woodside. *Case Study Research: Theory, Methods and Practice.* Emerald Group Publishing Ltd, UK, 2010.

[Yin03] R. K. Yin. *Case Study Research Design and Methods.* Thousand Oaks, California: Sage Publications, 2003.

[YLL+09] C.A. Yeung, I. Liccardi, K. Lu, O. Seneviratne, and T. Berners-Lee. Decentralization: The Future of Online Social Networking. In *In W3C Workshop on the Future of Social Networking Position Papers*, January 2009.

[YSl12] YSlow. Web Performance Best Practices and Rules @ONLINE., November 2012.

Human resource management in Slovak organizations in the context of contemporary tendencies – two decades in market economy

Zuzana Joniaková, Jana Blštáková, Michaela Vogl

University of Economics in Bratislava
Dolnozemská cesta 1
852 35 Bratislava
Slovakia
email: zuzana.joniakova@euba.sk, jana.blstakova@euba.sk, michaela.vogl@euba.sk

Abstract: Human resources are nowadays perceived as one of the most significant, key resource of company competitiveness in business environment. Business environment today is characteristic by constant on going changes which in increasing tendencies and are influencing every area of organization's business activity. Organizations today need to identify the challenges of new dimensions of their business activities and find ways to deal with them. The paper deals with the issue of approach changes to human resource management in organizations in dimensions, where these changes are applicable in order to participate on competitiveness of an organization. The paper also analyses the situation in Slovak organizations in readiness to face these changes.

1 Introduction

Human resources have been nowadays perceived as one of the key sources of organizational competitiveness. The ability to attract, retain and motivate high quality employees, the ability to form and develop their potential as well as the ability to manage their performance effectively, belongs among key challenges of human resource management in organizations. By force of personnel policies and many others depending activities, if realized professionally, it is possible to significantly contribute to total organizational performance. The demand on quality and professional approach changes influenced by external environment, which affect organizations in many aspects.

From the rather narrow perspective, we identify changes caused by exponentially speeding development in inventions in the world of technologies, which are further on followed by changes of sociological and demographical character. Especially these areas may be considered main source of important challenges for the area of human resource management, which personnel specialists nowadays need to deal with. However, this evokes also the change of perspective which an organization perceives its human resources management, as well as the change of way which personnel managers perceived their roles and contributions to overall success of their organization. This paper deals with the need of attitude changes to human resource management in organizations, examines ways which would lead to these changes and

also analyses contemporary situation of Slovak organizations from the aspect of readiness to demanded changes.

When it comes to Human Resource Management (HRM) development we must understand the enormous change caused by this transformation. In the centrally planed economy, there were personnel departments created in enterprises covering only administration. We can hardly talk about management here. The employees' performance, payroll, and attendance record in the workplace should have been included in their competencies. After the transformation, this understanding of the HR department's stature within a company had to be changed.

Slovakia has come through significant changes in its business environment in the last two decades. First it was the transformation of the National Economy System, from centrally planned to market economy in 1989. Later on, it was the creation of an independent state, the Slovak Republic in 1993. Now it is membership in the European Union in 2004, and preparation for the entrance to monetary union, planned for and realized in 2009.

These changes, especially the transformation process, had an essential impact on the everyday lives of Slovak citizens. A centrally planned economy brought many certainties and social safety for many future years.

Current HRM in Slovakia has been formed in the process where it is possible to identify three significant phases:

1. The conditions for starting this process were created after November the 17th 1989 as a consequence of the "Velvet Revolution", which lead to the transformation of national economy from centrally planned economy into market economy.
2. The second phase began with splitting the Czechoslovak Federative Republic into two separate republics in December 1992.
3. The third phase started with the entrance of the Slovak Republic into the European Union in May 2004.

Slovak organizations nowadays face the challenges identified in the text below. The way they've decided to deal with contemporary HRM tendencies, has been examined by force of continuous, systematic research. This research has gained international context in 2001, by joining the CRANET research group on HRM.

2 Changes in the approach to human resource management in organizations

Increasing speed of changes in the business environment evokes the need to leave old perceptions and used behavioral formulas, which have been developed, functioning and very useful in the past, but, became insufficient today. Based on a research carried out four years ago we have suggest to Slovak organizations to adopt European type of management, shaping HRM by transformation of personnel activities as the continuous transfer of delegation of operative tasks regarding HRM to line managers. Strategic planning, measuring and benchmarking – these activities will be

necessary to apply within the framework of HRM. Outsourcing of personnel activities is joined by monitoring effectiveness of particular activities of HRM. Some personnel activities will be excluded from the responsibility of HR departments and will be provided on commercially based external agencies. Personnel marketing as a tool for shaping and maintaining the required workforce, caused by the employees' good reputation and labor market research. An assessment centre is used, more often, as a method in shaping workforce of an organization. This method may be used in the process of selection, and as a method of managerial employee evaluation. Managing performance, we have defined as new strategic process enabling employees to understand what they should be orientated toward and what objectives should be reached. Permanent, lifelong education becomes necessary. Knowledge and information are becoming a preferred economic category in Slovakia also. They are very important factors of economic prosperity. Strengthening of collective bargaining began after the entrance of Slovakia into the EU. Even if the position of trade unions in many organizations has recently weakened as a consequence of many influences, we do believe in the continuous growth of trade union significance.

What we see now, it is the necessity to perceive human resource management according to its contribution to the success of the business of organization, which is different from the traditional approach where this area of management has been perceived as form of service delivering administrative agenda, mostly concerned rather with its processes and content than outcomes and contribution. Human resource management nowadays needs to obtain strategic character and becomes contributor to value added delivery for all subjects involved – organization, its employees as well as customers.

Readiness of organizations to instant reaction to fast speed of business environment changes is into great extant determined by its ability, which has Ulrich defined as the DNA of competitiveness [U09]. Meanwhile the "hard" skills, such as technologies, financial resources, etc. remain quite easy to assess and therefore influence, the problem appears in case of "soft" skills, the change of which is significantly more difficult.

These abilities of organizations depend on their employees' competencies, therefore the need of their redefinition is obviously an issue for human resource potential management. According to Ulrich, organizations nowadays aim their development aspirations within the area of "soft" skills into four areas, as follows:

- development of organizational credibility, based on trust in management and its decision,
- forthrightness, which expects removing barriers in communication in an organization as well as beyond its borders,
- maximization of flexibility, as the precondition of ability to adopt fast, to react fast to changes and even to be active in creating changes and inventing,
- investments into education and learning process, which would support the ability of fast reaction mentioned above.

Organizational credibility development needs to be perceived not only as part of public relation activity, but also as one of the main tools of employee loyalty enhancement and employee identification with the organization support. The contract of employees to their organization defined as relative force of identification of an individual with an organization consists of three components. One is the will to retain the membership in an organization, the other would be the belief in declared values and their acceptation as own, the consequence of which is the identification with employer's goals and finally the aim and will to deliver effort in order to these values application [A07].

Thus if an employee is devoted to an organization, which he or she works for, honors the opportunity and whishes to retain in the organization, its value system and its goals, also willing and prepared to work for the organization doing his/her best. Some authors even use the expression "citizen" of an organization. The commitment to the organization is supported by positive working experiences and inner factors, such as the level of trust, autonomy, working challenges, which are considered much more incentive compared to the external factors, such as wage and working conditions. The creation of trustfully atmosphere inside of the organization therefore might significantly support the feeling of employee dedication to the organization.

Organizations today are confronted with the concept of business ethics. Many of them has already implemented partial components of applied business ethics into their own business activities. This is happening by force of corporate social responsibility activities, which are very concrete steps towards development of satisfactory, long term, mutually beneficial relationship between organization and its environment. Systemic development of an ethical organization assumes healthy core, based on pillars of trust, freedom and responsibility. For many organizations may these values be still only a challenge, but many declare these values as principles of their business activities publically, or even as reasons and sources of their success in the role of an employer. In any case they remain a tool of organizations' credibility development influencing any involved partners in business.

The aim of forthrightness assumes to develop such an organization, where there will be all conditions for fluent information flow favorable on the vertical and horizontal line, as well as towards the inner and external environment of an organization. This shall enable the transfer of ideas and solutions without meaningless barriers and support business process in any level. It is possible to develop such skill by effective communication strategies.

Forms of communication in organizations, however, change depending on technical and technological development in the world of information technologies. Not only communication media change, but also the meaning of sharing information succumbs by these circumstances. Into human resource management has entered the concept of knowledge management and the question of delivering employees with high quality knowledge potential. Truneček has ten years ago spoken of moving from managing human resources to managing human knowledge potential [ST03]. Knowledge management brings many new challenges into personnel management in general. Information technologies has so far remain support tool for HR managers in their

administrative agenda, while knowledge management challenges forces them to move on towards the centre of data-information-knowledge-wisdom chain[T03]. Also external situation forces organizations to optimize their processes, decrease their expenses, which may, for example in the area of information management, be very effectively supported by application of self-service information technologies for personnel management. These technologies delegate maximum of operative activities to employees, which leads to involving them into human resources processes, helping faster and flexible information flow within the organization. All necessary changes meanwhile evoke pressures on human potential quality. Thus the aim of contemporary management becomes the development of organizational system, within which the employee development takes significant place in order to reach quality, effectiveness and competitiveness of an organization [M09].

Contemporary perception of an employee and its role within an organization, which has been developed by the concept of knowledge management, moves the core of human resource management towards the top management of an organization. From the position of strategic partner it is possible to work on the concept of personnel strategy, which supports forthrightness, mutual information sharing and enrichment of information sources. On the other hand the encouragement to sharing and open communication might nowadays be accepted only with difficulties, for the great value of quality information sources. The support in working with information shall therefore be also a challenge within corporate culture development, which ought to be perceived as significant tool for corporate strategy implementation. Corporate culture reflects inner consistency, containing employees' attitudes influencing their behavior in order to reaching organizational goals set [K10]. In case the strategy is elaborated into reasonable and understandable goals and procedures how to reach the goals, and these are properly communicated to the employees, there has been a premise of its successful implementation and employees' identification created. If this strategy also brings desired and visible results, the way of delivering organizational performance and working behavior becomes the appropriate one and considered as profitable, therefore willingly accepted it becomes content of corporate culture and supports the strategy. The compliance of corporate strategy and corporate culture has become one of the preconditions of long term successfulness of an organization.

The speed of environmental changes contemporary increases and intensifies which is a factor that all organizations need to face. The more successful organizations are able to react instantly by developing an ability to learn from changes, instead of trying to control and master the change. As a consequence of these changes, organizations need to run constant revision of procedures and programs, transformation of processes and changes in corporate culture. This changes any perception of whole organization as well as the self-perception. Human resource managers ought to be the once who are able to support organizational abilities to adapt for all types of changes. Even if all models of change management are theoretically elaborated into details, their practical utilization often doesn't bring expected results. Ulrich stats following most frequent reasons of change failure [U09]:

- lack of linkage to the strategy,
- considering changes a fashion issue of fast solution,

- short term perception,
- policy, compromising the change,
- overestimated expectation in contrary to poor results, inflexibility,
- insufficient management of change,
- concerns of unknown,
- inability to mobilize loyalty and engagement for change realization.

Successful realization of changes in an organization is obviously supported by processes of consequent learning and development. It is not only the processes of employee education and development, as they have been perceived by traditional personnel management, but everyday sharing of information and mutual enrichment new knowledge, emerging out of the organization's activities. Because as the primary incentive for changes realization are the organizational external influences, the primary determinants of their successful implementation are people inside the organization [BM93]. Their ability to learn from experiences in the process of changes application supports the efficiency of whole organization. Learning ability of individuals and whole organizations is conditioned by effective communication, support of individual expression and trust [A07]. This further on supports devotion of organization's visions and willingness of its employees to accept and realize decisions, reacting to environmental changes as to an opportunity that it creates. This leads to the essence of linking all above mention areas of building organizational skills, which lead into support of synergic effect of mutual influence.

3 The analysis of contemporary situation in Slovak organizations

The situation in the area of human resource management practice in Slovak organization has been an target of monitor at annual basis, realized within the framework of an international research collaboration Cranet (The Cranfield Nework - CRANET), coordinated by the Cranfield School of Management. Permanently gathered information regarding policies and practically applied tools of human resource management in Slovak organizations has become proven track record of collecting powerful, representative data, on a continuing basis; undertaking rigorous analysis and disseminating high quality results. On such platform we are able to evaluate the situation in analyzed area in the practice of Slovak organization and confront these finding with tendencies identified within international concept.

We have used the Ulrich's conception of organizational "soft" skills, i.e. credibility, forthrightness, flexibility and knowledge orientation introduced above, as the basis for analyzing personnel procedures and policies in the context of their implication to competitiveness. Ulrich has identified these organizational competencies and defined them as the core of the DNA of organizational competitiveness, meanwhile their development and utilization is directly dependent on managing human resources. For evaluation of the reaction ability of Slovak organization for contemporary challenges of business environment, examining applied personnel procedures and programs, it is essential to focus on development of above mention distinguished skills.

The analytical part of the paper is based on the survey data output, the context of which has already been explained above, realized at the Department of Management, at the University of Economics in Bratislava. The main aim has been to verify the extent into which organizations in Slovakia choose the personnel management measures and procedures, which would indicate their disposal of distinguished skills or at least potential to develop these skills in the future. The main assumption has been the dependence of choices in "hard" measures on the level of "soft" skills development. As the basis presumption we have chosen to focus on the formalized status of human resource manager within an organization. We have assumed that organizations having their human resource manager present in the body of top management, also formalized within the hierarchy, will be in greater extent displaying their distinguished skills by choice of relevant personnel policies and application of subsistent personnel practices, both oriented towards credibility and forthrightness of their organization. Also we have assumed that these organizations will be aiming to reach high dynamics of their processes, inventive approach and reaction time minimizing need to change application. Among these organizations the flexibility support has been expected by employee education and training concept application with character of learning organization.

We have also explored the tendency of the need to formalize human resource managers' status within top managerial levels of decision-making process from the chronological aspect (chart 1). Based on the results, we may note, that organizations accept the implication of formally having HR managers on strategic levels, based on the fact that the number of organizations which do not do so has declined down to fifty percent during past seven years.

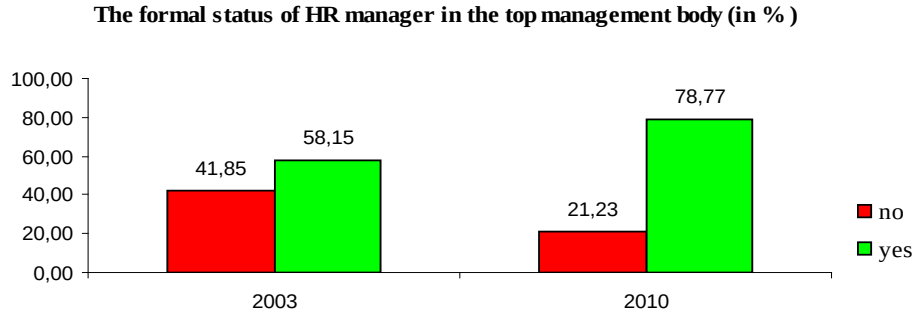


Chart 1: The tendency of formal involvement of HR manager in organizations' top managements

Formal increase of the importance of human resource departments in organizations prove the change in perceiving the purport of human potential to organizational competitiveness and introduces an appeal upon the human resources management quality improvement. Creation of opportunities to participate on strategic level of decision-

making process within an organization may be considered essential precondition for becoming the strategic partner in business, however the status itself oughtn't to be perceived the goal of HR departments either the guarantee of their performance quality increase.

Thus we assume differences in particular personnel measures and procedures, which develop abilities participating on development of organizational competitiveness, based just on the formalized status of human resource manager in top management. By analyzing formulated challenges for the period of following three years, based in the research results, we need to establish the finding, that organizations, which have their HR managers involved into top managements, tent to articulate their appeal on excellent HR services and to transform this area of management into strategic partnership and business partnership, worthily contributing to reaching strategic goals of their organization. Among these organizations we have more often noticed the requirement of organizational culture transformation, emphasizing values such as politeness, fairness, dignity. They also feel the need to reinforce the participation on decision-making across their organizational structure and also the need to formulate and introduce into utilization ethical codex, which would reflect all above stated intentions. We have also found out, that all organizations which have formalized status of their HR managers in top management bodies would more tend to their future expectation and orientate their management direction into long term perspective, having their up coming challenges indentified more often.

In total, among most frequently stated challenges, which organizations in analyzed sample have mentioned as challenges for up coming three years, the need of personnel processes quality increase has appeared quite often.

Evaluating the issue of challenge setting we have determined following areas, according to challenges identified in human resource management in organizations for up coming three years:

- employee retention, organizations have identified the need to optimize the structure of their employees, providing their quality, developing their competencies and reliability, quite often also the term core employees has been mentioned,
- creation of complex systems of employee assessment and performance management, where in organizations with HR management participating in top management level, also appears the request of linkage between performance management system and business performance
- complex employee development and education system, where the organizations plan to focus on talent management and its linkage to career growth.

Besides these intentions there is still as a challenge perceived the need to develop and in

greater extent utilize the potential of information technologies linked to application supporting other managerial subsystems within an organization. Many organizations have also expressed the need to reevaluate their compensation systems, especially in the area of benefits and intensify their employees' motivation issue.

The research results show that formulation of future intentions and formalization of these intentions in the way of strategic documentation, such as corporate strategy and

corporate values, is an issue where we can notice different approach of organizations which have their human resource manager in the top management board and those which hasn't (chart 2).

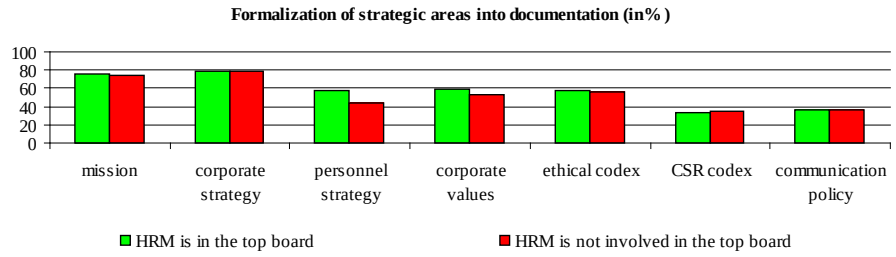


Chart 2: Comparison of strategic areas formalization into organizational documentation

However, by more detailed analysis of other practical personnel procedures and processes reflecting development of distinguished skills, we have surprisingly found out very little or even irrelevant differences between approaches of both analyzed groups of organizations. Based on this findings, we need to make conclusion, that formalization of the human resource managers' status in the organizations' bodies of top managerial levels, aiming to increase the HRM quality, might be considered foundation, but must not be perceived guarantee of developing organizational competitive skills. By this status created options to participate on the strategic decisions needs to be supported by HR managers and utilized more intensively, but also valorized in favor of quality of their tactical and operative procedures, so that the reason of such status would be valid and proofed. However the formalization and declaration of human potential importance in an organization ought to be, on the contrary, the result of practical application values which declare this meaning. Further on, we have therefore focused on analyzing concrete personnel procedures, which directly support development of credibility, forthrightness, flexibility and learning competencies of organizations, where we have left the selection of analyzed sample according to the status of HR manager in the top management, since the differences between approaches hadn't appeared remarkable.

Credibility of an organization is supported by the way of organization presents itself, and its message to the external environment as well as the attitude towards its employees. One of the ways of sending the message is forming and communication of the values, which an organization find essential and which they stick to by any of their activities. Therefore we have we have examined the credibility development of Slovak organizations by analyzing formulated values within their corporate culture, focusing especially on the way of their declaration, implementation and communication (chart 3). In analyzed sample of analyzed organizations we have noticed among most frequently declared values responsible approach, efficiency, quality aim and team sprit. These are mostly values emphasizing orientation towards performance; meanwhile with significantly lower frequency organizations declare trust, respect, recognition, safety, integrity, activity and dynamic as their desired values. These are the values characteristic for partnership approach and creation of the atmosphere of trust within the approach to

employees. These values still remain underestimated, or considered values useless for business competitiveness development, or are meant for more suitable for the NGOs.

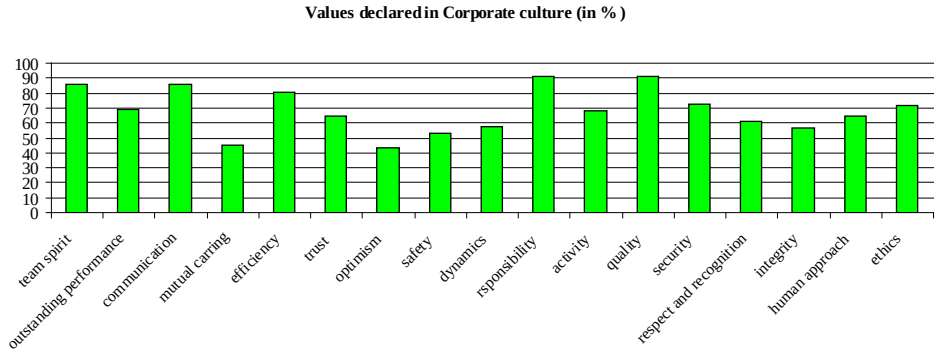
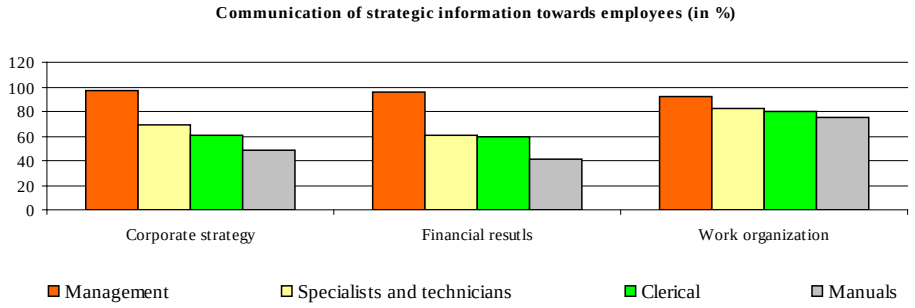


Chart 3: Values declared in corporate culture

Open organizations towards their information flow means to approach to information management in order to maximize the elimination of various barriers and obstructions, enabling, fast and efficient information flow of any direction within an organization as well as towards its environment. The object of interest researching this issue within the sample of organizations have been communication process, their character and used communication tools. The basis for analysis has been examination of the intensity of sharing strategic information regarding corporate culture, financial results and work organization with various categories of employees (chart 4).



.

Chart 4: Sharing strategic information with employees according to their categories

Intensity of communication and the extent of information delivery among all involved employees are slightly higher in the pool of organizations, where human resource manager is involved into top management level, but this difference may be considered irrelevant, since it is only approximately 10%.

In case organizations aim to support their employees' identification with its values and goals, they need to be involved and not only information must be easily accessible, but also purposely communicated. In examined areas the most communicated strategic information has been information about work organization towards all categories of employees. Reasonably theses information directly influence employees working performance, but even here we observe the average 80%, naturally expected 100%. Information regarding strategic goals and choices are less shared with employees, significantly dropping by the decrease of the level of managerial responsibilities of employees. Further on employees are provided with the feedback in the form of financial results of an organization, again dependent of the level of their managerial responsibility within organizational hierarchy and appears to be approximately between 30-60%. We consider these results not very favorable, because they prove rather low level of sharing essential information, which doesn't positively influence development of the environment supporting employees' involvement and their identification with corporate goals.

The abilities of organizations to share knowledge by force of open communication also may be examined by the focus on top management communication of their ideas and aims towards employees (top down) (chart 5), as well as the communication of employees issues towards their subordinates of any level (bottom up).

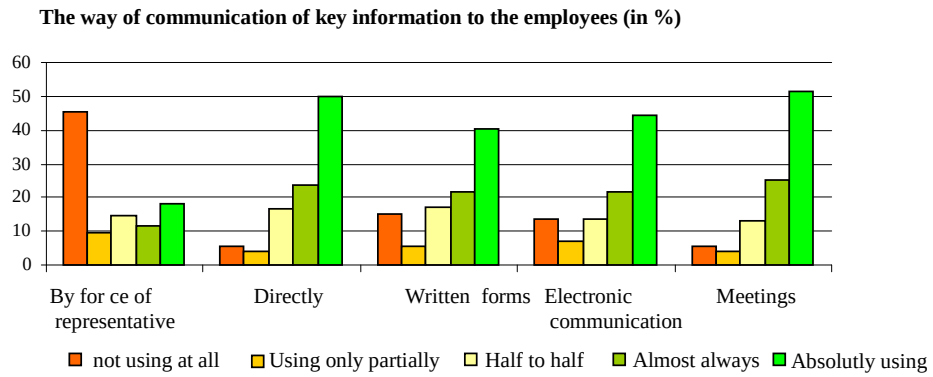


Chart 5: Communication of key information towards employees (top-down)

The communication top down is mostly realized directly by means of verbal forms, but also the written forms of communication are quite frequent and of course electronic media are being used, however 15% of organizations within the sample consider this form unsuitable for communicating key information to their employees. Very common forms of communication remain meetings and various assemblies. Because the communication via employee representative body or other formal spear for employees needs, is being used only very little, or not at all, we may state that organizations prefer to communicate their key information towards their employees using direct forms of communication, avoiding mediator or representative.

However to communication on the bottom up level, various forms of briefings and meetings are quite popular.

Even if not very common, but there are still present communication cannels which create barriers, or makes for employees less possible to communicate with top management directly, and might result into gaining the feeling of frustration from ignorance or lack of interest. This disturbs development of a climate favorable to employees' involvement into organizational matters. Direct communication between employees and senior management has been stated as supported only in 12% of organization from the sample. Forms of communication supporting various forms of employees' participation on decision making process, such as system of innovation ideas, remains less applied (13%). We find remarkable that forms of electronic communication are significantly more frequent in top down direction compared to bottom up line, where we've noted only half of the „top-down" intensity. This finding proves that the "one way" form of communication still majors in many organizations, which is controversial feature of communication policy aiming to support positive environment for sharing information, ideas and know-how.

Open communication and continuous education and development are coherent competencies and their development is mutually dependent. We have considered information technologies the "hard" skills of communication flow support in organizations and we have focused on the use of IT in personnel management practice. Since fast, easy and impeccable information and knowledge sharing, might be significantly supported by customized information systems, we have analyzed personnel processes which were actually using this support in organizations. As mentioned above, improvement and integration of personnel information systems with other managerial information systems still remain a challenge for many organizations in Slovakia for upcoming period of three years. This demand we find legitimate, because as the results show, information technologies support is being used in the significant extent for wage agenda (94%). For education and training activities support the information technologies find their utilization only in less than one third of the sample, and only one third use IT to communicate information regarding their human resource process and policies.

Flexibility of organizations and their readiness to react to contemporary changes might be in the area of human resource management supported by HR processes flexibility. However flexibility as the desired competency of competitive organization also reflects in very concrete practical tools, such as work organization. Concretely, we have analyzed various models of flexible work regimes application, which have been relatively little used in comparison to European Union Standards. Based on our research we may note, that traditional work regime, such as shifts, or overtime working hours are quite common. More than a half of organizations have already gotten familiar with flexible regimes application, however the will to involve newer or more progressive forms remains vague. Work regimes, such as job sharing, compressed weeks or tele-work are mentioned by only 10-20% of organizations as applied for less than 5% of their employees.

Above mentioned flexible work regimes are contemporary involved into personnel strategies of organizations abroad to build a concept of reaction to negative crises impact, these organizations report positive experience. Inability to utilize these work regimes within the work design in Slovak organizations indicates difficulties with their flexibility in personnel processes and in other areas as well.

4 Conclusion

The analysis of contemporary situation in Slovak organizations proves the fact, that formalization of the human resource manager status with the top management doesn't automatically guarantee neither increase of quality of personnel processes nor their contribution to organizational competitiveness. The finding, that quality of personnel processes is independent from such status formalization, might on one hand appear shocking on the other hand indicates that managing human resources ought to be no more concentrated into hands of few specialists, but shall be the concern of any active subject of management at any hierarchical level. However, it is quite essential to realize the contribution of quality personnel processes and the advocate and carrier of such idea does not necessary be present only in top management. On the other hand research results have proved the fact that there is certain inability of HR managers to accept and utilize the role of strategic partner, which they in many cases need to handle. Quite often they are not able to take advantage of such status and use this trust and power to co-create the added of their organization. Thus in the role of change agents, HR manager often fail or even become target of disappointment.

What shall be the role of personnel managers by forming key competencies of organizations? To be able to transform employees' individual abilities into abilities of whole organization, which would remain competitive, it is necessary to continuously monitor these skills and to have actual review about what competencies the organization and its employees dispose of. Naturally it is insufficient to be in continuous contact with present situation in organizational predispositions and competencies; they must be predicted, estimated, expected and accepted. Thus it is necessary to identify, define and acquire these competencies in order to be able to harmonize them with corporate strategy and further on to utilize them properly and fully. The aim is to effectively utilize these developed competencies; otherwise any work with them might become useless personnel management activity. Based on Ulrich, skills are the link between strategy and its realization [U09]. Following step would be preparation of human resources management policies and procedures, which would form desired strategic goals into operative actions in various HR functions. Very crucial expectation from personnel managers is their ability to create relevant indicators of organizational skills and competencies monitor. This will enable to examine efficiency and effectiveness of sources used in this area of management as well as to declare its contribution to business activities of the whole organization. The difficulty of this task is proved by the fact that 75% of organizations declare unsuccessful development of new distinguished organizational competencies [U09]. Difficulty to develop „soft"organizational skills shall not be a factor discouraging personnel specialists to try hard in this area, on the contrary it ought to be perceived as great challenge leading towards the participation on competitiveness development of their organization.

References

[1] Ulrich, D. Mistrovské řízení lidských zdrjů. Praha, Grada 2009. 272s. ISBN 978-80-247-3058-5. s.29

[2] Arnold, J. a kol. Psychologie práce. Brno, Computer Press 2007. 629s. ISBN 978-80-25-1518-3. s.259
[3] Spracované podľa: Sveiby, E.K.1997. In: Truneček, J. 2003. *Znalostní podnik ve znalostní společnosti*. Praha: Professional publishing, 2003. 312 s., ISBN 80-86419-35-5, s. 151
[4] Truneček, J. 2003. *Znalostní podnik ve znalostní společnosti*. Praha: Professional publishing, 2003. 312 s., ISBN 80-86419-35-5, s. 153
[5] Spracované podľa: : Majtán, M. 2009. *Manažment. Bratislava.* Bratislava: Sprint, 2009. 405s., ISBN 978-80-89393-07-7, s.264
[6] Kachaňáková, A. 2010. *Organizačná kultúra*. Bratislava: IuraEdition, 2010. 142 s., ISBN 978-80-8078-304-4, s.113
[7] Ulrich, D. Mistrovské řízení lidských zdrjů. Praha, Grada 2009. 272s. ISBN 978-80-247-3058-5. s.169
[8] Benjamin, G. & Mabey, C. (1993), "Facilitating Radical Change", In: Maybe, C. & Mayon-White, B. (eds.), Managing Change (2nd ed), London: Paul Chapman, s181
[9] Arnold, J. a kol. Psychologie práce. Brno, Computer Press 2007. 629s. ISBN 978-80-25-1518-3. s.588
[10] Ulrich, D. Mistrovské řízení lidských zdrjů. Praha, Grada 2009. 272s. ISBN 978-80-247-3058-5. s.203
[11] Ulrich, D. Mistrovské řízení lidských zdrjů. Praha, Grada 2009. 272s. ISBN 978-80-247-3058-5. s.29