BALTIC CONFERENCE

Advanced Topics in

Telecommunication

Tartu, 07.08. - 22.08.2009

Universität Rostock 2009

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

Erstellung der Druckvorlage:
Sebastian Engel

Entwurf des Umschlagbildes:
Dr. Christine Bräuning

CIP-Kurztitelaufnahme:

ISBN:

Bezugsmöglichkeiten:

Universität Rostock
Institut für Informatik
Frau Kerstin Krause
Albert-Einstein-Straße 21
18059 Rostock

Universität Rostock
Wissenschaftsverbund IuK
Frau Dr. Christine Bräuning
Albert-Einstein-Straße 21
18059 Rostock

Druck: Universitätsdruckerei Rostock

Table of Contents

Preface

BaSoTI is facing a successful development, going into its fifth year, with the associated conference going into its third year.

It was in 2005, that the University of Bremen, the University of Lübeck, the ISNM - International School of New Media at the University of Lübeck, 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 (DAAD - Deutscher Akademischer Austausch Dienst), a series of lectures was offered between August 1st and August 14th, 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 program, BaSoTI 2 was again held at Vilnius, from July 31st to August 14th, 2006, BaSoTI 3 took place in Riga, Latvia at the Information Systems Management Institute, from August 26th to September 10th, 2007, BaSoTI 4 was held at the University of Tartu, Estonia, from August 8th to August 23rd, 2008, and BaSoTI 5 took place in Tartu, Estonia again, from August 7th to August 22nd. Presently BaSoTI 6 is planned for August 2010 in Kaunas, Lithuania.

Since BaSoTI 3, the Summer School lectures have been complemented by a one day scientific event on Advances in Telecommunications. 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.

The present proceedings give proof of the research results submitted by the participants and lecturers of BaSoTI 5.

Clemens H. Cap
Rostock, October 2009.

Program Committee

Andreas Ahrens (University of Applied Sciences, Wismar)
Clemens Cap (University of Rostock)
Karl-Dirk Kammeyer (University of Bremen)
Andreas Könsgen (University of Bremen)
Thomas Mundt (University of Rostock)
Andreas Schrader (ISNM Lübeck)
Peter Sobe (University of Lübeck)
Satish Srirama (University of Tartu)
Karsten Wolf (University of Rostock)
Dirk Wübben (University of Bremen)

Performance Analysis of SVD-assisted Broadband MIMO Transmission Schemes

John-Eric Kamps, Andreas Ahrens
Hochschule Wismar, University of Technology, Business and Design
john-eric.kamps@hs-wismar.de, andreas.ahrens@hs-wismar.de

Mosa Ali Abu-Rgheff
University of Plymouth
mosa@plymouth.ac.uk

Abstract

Since the capacity of multiple-input multiple-output (MIMO) systems increases linearly with the minimum number of antennas at both, the transmitter as well as the receiver side, MIMO schemes have attracted a lot of attention. However, non-frequency selective MIMO links have reached a state of maturity. By contrast, frequency selective MIMO links require substantial further research, leading in this contribution to a joint optimization of the number of activated MIMO layers and the number of bits per symbol along with the appropriate allocation of the transmit power under the constraint of a given fixed data throughput. Our results show that in order to achieve the best possible bit-error rate, not necessarily all MIMO layers have to be activated.

1 Introduction

In order to comply with the demand on increasing available data rates in particular in wireless technologies, systems with multiple transmit and receive antennas, also called MIMO systems (multiple-input multiple-output), have become indispensable and can be considered as an essential part of increasing both the achievable capacity and integrity of future generations of wireless systems [16, 23]. In general, the most beneficial choice of the number of activated MIMO layers and the number of bits per symbol along with the appropriate allocation

of the transmit power offer a certain degree of design freedom, which substantially affects the performance of MIMO systems. The well-known water-filling technique is virtually synonymous with adaptive modulation [24] and it is used for maximizing the overall data rate. However, delay-critical applications, such as voice or streaming video transmissions, may require a certain fixed data rate. For these fixed-rate applications it is desirable to design algorithms, which minimize the bit-error rate (BER) at a given fixed data rate.

Assuming perfect channel state information, the channel capacity can only be achieved by using water-pouring procedures. However, in practical application only finite and discrete rates are possible. Therefore in this contribution the efficiency of fixed transmission modes is studied regardless of the channel quality. However, non-frequency selective MIMO links have attracted a lot of research and have reached a state of maturity [5]. By contrast, frequency selective MIMO links require substantial further research, where spatio-temporal vector coding (STVC) introduced by RALEIGH seems to be an appropriate candidate for broadband transmission channels, where multipath propagation is no longer a limiting factor in data transmission [20, 21, 1]. Against this background, the novel contribution of this paper is that we demonstrate the benefits of combining a suitable choice of activated MIMO layers and number of bits per symbol along with the appropriate allocation of the transmit power under the constraint of a given data throughput.

The remaining part of this paper is organized as follows: Section 2 introduces the system model and the considered quality criteria are briefly reviewed in section 3. The proposed solutions of bit and power allocation are discussed in section 4, while the associated performance results are presented and interpreted in section 5. Section 6 provides some concluding remarks.

2 Broadband MIMO system model

When considering a frequency selective MIMO link, composed of n_{T} transmit and n_{R} receive antennas, the block-oriented system is modelled by

$$\mathbf{u} = \mathbf{H} \cdot \mathbf{c} + \mathbf{w} \ . \tag{1}$$

In (1), $\mathbf{c}$ is the $(N_{\mathrm{T}} \times 1)$ transmitted signal vector containing the complex input symbols transmitted over n_{T} transmit antennas in K consecutive time slots, i. e., $N_{\mathrm{T}} = K\, n_{\mathrm{T}}$. This vector can be decomposed into n_{T} antenna-specific signal vectors $\mathbf{c}_\mu$ according to

$$\mathbf{c} = \left(\mathbf{c}_1^{\mathrm{T}}, \ldots, \mathbf{c}_\mu^{\mathrm{T}}, \ldots, \mathbf{c}_{n_{\mathrm{T}}}^{\mathrm{T}}\right)^{\mathrm{T}} \ . \tag{2}$$

In (2), the $(K \times 1)$ antenna-specific signal vector $\mathbf{c}_\mu$ transmitted by the transmit antenna μ (with $\mu = 1, \ldots, n_\mathrm{T}$) is modelled by

$$\mathbf{c}_\mu = (c_{1\,\mu}, \ldots, c_{k\,\mu}, \ldots, c_{K\,\mu})^\mathrm{T} \quad . \tag{3}$$

The $(N_\mathrm{R} \times 1)$ received signal vector $\mathbf{u}$, defined in (1), can again be decomposed into n_R antenna-specific signal vectors $\mathbf{u}_\nu$ (with $\nu = 1, \ldots, n_\mathrm{R}$) of the length $K + L_\mathrm{c}$, i. e., $N_\mathrm{R} = (K + L_\mathrm{c})\, n_\mathrm{R}$, and results in

$$\mathbf{u} = \left(\mathbf{u}_1^\mathrm{T}, \ldots, \mathbf{u}_\nu^\mathrm{T}, \ldots, \mathbf{u}_{n_\mathrm{R}}^\mathrm{T}\right)^\mathrm{T} \quad . \tag{4}$$

By taking the $(L_\mathrm{c} + 1)$ non-zero elements of the resulting symbol rate sampled overall channel impulse response between the μth transmit and νth receive antenna into account, the antenna-specific received vector $\mathbf{u}_\nu$ has to be extended by L_c elements, compared to the transmitted antenna-specific signal vector $\mathbf{c}_\mu$ defined in (3). The $((K + L_\mathrm{c}) \times 1)$ signal vector $\mathbf{u}_\nu$ received by the antenna ν (with $\nu = 1, \ldots, n_\mathrm{R}$) can be constructed, including the extension through the multipath propagation, as follows

$$\mathbf{u}_\nu = \left(u_{1\,\nu}, u_{2\,\nu}, \ldots, u_{(K+L_\mathrm{c})\,\nu}\right)^\mathrm{T} \quad . \tag{5}$$

Similarly, in (1) the $(N_\mathrm{R} \times 1)$ noise vector $\mathbf{w}$ results in

$$\mathbf{w} = \left(\mathbf{w}_1^\mathrm{T}, \ldots, \mathbf{w}_\nu^\mathrm{T}, \ldots, \mathbf{w}_{n_\mathrm{R}}^\mathrm{T}\right)^\mathrm{T} \quad . \tag{6}$$

The vector $\mathbf{w}$ of the additive, white Gaussian noise (AWGN) is assumed to have a variance of U_R^2 for both the real and imaginary parts and can still be decomposed into n_R antenna-specific signal vectors $\mathbf{w}_\nu$ (with $\nu = 1, \ldots, n_\mathrm{R}$) according to

$$\mathbf{w}_\nu = \left(w_{1\,\nu}, w_{2\,\nu}, \ldots, w_{(K+L_\mathrm{c})\,\nu}\right)^\mathrm{T} \quad . \tag{7}$$

Finally, the $(N_\mathrm{R} \times N_\mathrm{T})$ system matrix $\mathbf{H}$ of the block-oriented system model, introduced in (1), results in

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_{1\,1} & \cdots & \mathbf{H}_{1\,n_\mathrm{T}} \\ \vdots & \ddots & \vdots \\ \mathbf{H}_{n_\mathrm{R}\,1} & \cdots & \mathbf{H}_{n_\mathrm{R}\,n_\mathrm{T}} \end{bmatrix} \quad , \tag{8}$$

and consists of $n_\mathrm{R}\, n_\mathrm{T}$ single-input single-output (SISO) channel matrices $\mathbf{H}_{\nu\,\mu}$ (with $\nu = 1, \ldots, n_\mathrm{R}$ and $\mu = 1, \ldots, n_\mathrm{T}$). The system description, called spatio-temporal vector coding (STVC), was introduced by Raleigh and can also be seen as an extension of the data directed estimation (DDE) introduced by Hsu [11]. Each of theses matrices $\mathbf{H}_{\nu\,\mu}$ with the dimension $((K + L_\mathrm{c}) \times K)$ describes the influence of the channel from transmit antenna μ to receive antenna ν including transmit and receive filtering. The channel convolution matrix $\mathbf{H}_{\nu\,\mu}$ between the μth transmit and νth receive antenna is obtained by taking the

$(L_\mathrm{c}+1)$ non-zero elements of resulting symbol rate sampled overall impulse response into account and results in:

$$\mathbf{H}_{\nu\,\mu} = \begin{bmatrix} h_0 & 0 & 0 & \cdots & 0 \\ h_1 & h_0 & 0 & \cdots & \vdots \\ h_2 & h_1 & h_0 & \cdots & 0 \\ \vdots & h_2 & h_1 & \cdots & h_0 \\ h_{L_\mathrm{c}} & \vdots & h_2 & \cdots & h_1 \\ 0 & h_{L_\mathrm{c}} & \vdots & \cdots & h_2 \\ 0 & 0 & h_{L_\mathrm{c}} & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & h_{L_\mathrm{c}} \end{bmatrix} . \tag{9}$$

Throughout this paper, it is assumed that the $(L_\mathrm{c}+1)$ channel coefficients, between the μth transmit and νth receive antenna have the same averaged power and undergo a Rayleigh distribution. Furthermore, a block fading channel model is applied, i. e., the channel is assumed to be time invariant for the duration of one SDM (spatial division multiplexing) MIMO data vector.

The interference, which is introduced by the off-diagonal elements of the channel matrix $\mathbf{H}$, requires appropriate signal processing strategies. A popular technique is based on the singular-value decomposition (SVD) [10] of the system matrix $\mathbf{H}$, which can be written as $\mathbf{H} = \mathbf{S} \cdot \mathbf{V} \cdot \mathbf{D}^\mathrm{H}$, where $\mathbf{S}$ and $\mathbf{D}^\mathrm{H}$ are unitary matrices and $\mathbf{V}$ is a real-valued diagonal matrix of the positive square roots of the eigenvalues of the matrix $\mathbf{H}^\mathrm{H}\,\mathbf{H}$ sorted in descending order. The transpose and conjugate transpose (Hermitian) of $\mathbf{D}$ are denoted by $\mathbf{D}^\mathrm{T}$ and $\mathbf{D}^\mathrm{H}$, respectively. The SDM MIMO data vector $\mathbf{c}$ is now multiplied by the matrix $\mathbf{D}$ before transmission. In turn, the receiver multiplies the received vector $\mathbf{u}$ by the matrix $\mathbf{S}^\mathrm{H}$. Thereby neither the transmit power nor the noise power is enhanced. The overall transmission relationship is defined as

$$\mathbf{y} = \mathbf{S}^\mathrm{H}\,(\mathbf{H} \cdot \mathbf{D} \cdot \mathbf{c} + \mathbf{w}) = \mathbf{V} \cdot \mathbf{c} + \tilde{\mathbf{w}}\,. \tag{10}$$

As a consequence of the processing in (10), the channel matrix $\mathbf{H}$ is transformed into independent, non-interfering layers having unequal gains.

3 Quality criteria

In general, the quality of data transmission can be informally assessed by using the signal-to-noise ratio (SNR) at the detector's input defined by the half vertical eye opening and the noise power per quadrature component according to

$$\varrho = \frac{(\text{Half vertical eye opening})^2}{\text{Noise Power}} = \frac{(U_\mathrm{A})^2}{(U_\mathrm{R})^2}\ , \tag{11}$$

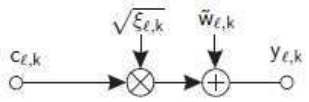

Fig. 1: *Resulting layer-specific SDM MIMO system model (with $\ell = 1, 2, \cdots, L$ and $k = 1, 2, \cdots, K$)*

which is often used as a quality parameter [4]. The relationship between the signal-to-noise ratio $\varrho = U_{\mathrm{A}}^2 / U_{\mathrm{R}}^2$ and the bit-error probability evaluated for AWGN channels and M-ary Quadrature Amplitude Modulation (QAM) is given by [13, 19]

$$P_{\mathrm{BER}} = \frac{2}{\log_2(M)} \left(1 - \frac{1}{\sqrt{M}}\right) \operatorname{erfc}\left(\sqrt{\frac{\varrho}{2}}\right) \quad . \tag{12}$$

When applying the proposed system structure, the SVD-based equalization leads to different eye openings per activated MIMO layer ℓ (with $\ell = 1, 2, \cdots, L$) at the time k (with $k = 1, 2, \cdots, K$) within the SDM MIMO signal vector according to

$$U_{\mathrm{A}}^{(\ell,k)} = \sqrt{\xi_{\ell,k}} \cdot U_{\mathrm{s}\,\ell} \quad , \tag{13}$$

where $U_{\mathrm{s}\,\ell}$ denotes the half-level transmit amplitude assuming M_ℓ-ary QAM and $\sqrt{\xi_{\ell,k}}$ represents the corresponding positive square roots of the eigenvalues of the matrix $\mathbf{H}^{\mathrm{H}}\,\mathbf{H}$ (Fig. 1). The layer-specific weighting factors are analyzed in

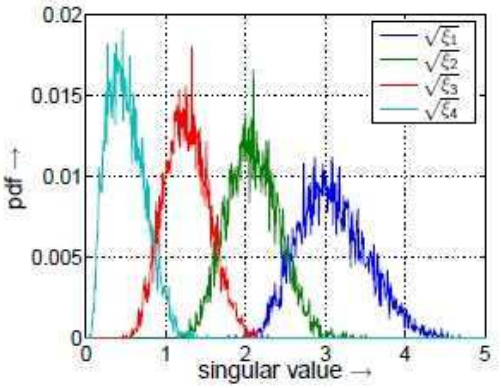

Fig. 2: *PDF (probability density function) of the layer-specific amplitudes $\sqrt{\xi_\ell}$ (with $\ell = 1, 2, \cdots, 4$ and $L_{\mathrm{c}} = 1$)*

Fig. 2 and 3 for different parameters of L_{c}. Taking frequency selective MIMO links rather than non-frequency selective MIMO links into account, large delay-spreads seems to be highly beneficial and lead to further degree of design freedom

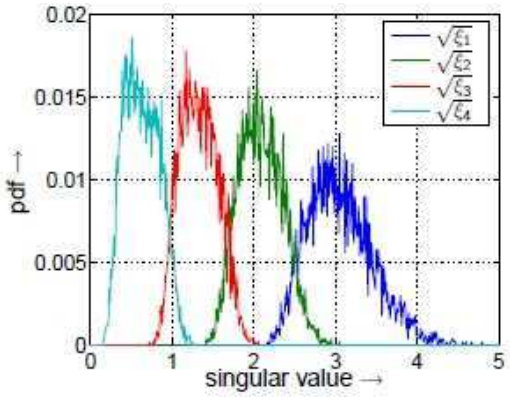

Fig. 3: *PDF (probability density function) of the layer-specific amplitudes* $\sqrt{\xi_\ell}$ *(with* $\ell = 1, 2, \cdots, 4$ *and* $L_\mathrm{c} = 4$*)*

as investigated in [17] or [8]. Together with the noise power per quadrature component, the SNR per MIMO layer ℓ at the time k becomes

$$\varrho^{(\ell,k)} = \frac{\left(U_\mathrm{A}^{(\ell,k)}\right)^2}{U_\mathrm{R}^2} = \xi_{\ell,k}\,\frac{(U_{\mathrm{s}\,\ell})^2}{U_\mathrm{R}^2} \quad . \tag{14}$$

Using the parallel transmission over $L \leq \min(n_\mathrm{T}, n_\mathrm{R})$ MIMO layers, the overall mean transmit power becomes $P_\mathrm{s} = \sum_{\ell=1}^{L} P_{\mathrm{s}\,\ell}$, where the number of readily separable layers[1] is limited by $\min(n_\mathrm{T}, n_\mathrm{R})$. Considering QAM constellations, the average transmit power $P_{\mathrm{s}\,\ell}$ per MIMO layer ℓ may be expressed as [7, 14, 19]

$$P_{\mathrm{s}\,\ell} = \frac{2}{3}\,U_{\mathrm{s}\,\ell}^2\,(M_\ell - 1) \quad . \tag{15}$$

Combining (14) and (15), the layer-specific SNR at the time k results in

$$\varrho^{(\ell,k)} = \xi_{\ell,k}\,\frac{3}{2\,(M_\ell - 1)}\,\frac{P_{\mathrm{s}\,\ell}}{U_\mathrm{R}^2} \quad . \tag{16}$$

In order to transmit at a fixed data rate while maintaining the best possible integrity, i. e., bit-error rate, an appropriate number of MIMO layers has to be used, which depends on the specific transmission mode, as detailed in Tab. 1. In general, the BER per SDM MIMO data vector is dominated by the specific transmission modes and the characteristics of the singular values, resulting in different BERs for the different QAM configurations in Tab. 1. An optimized adaptive scheme would now use the particular transmission modes, e. g., by using bit auction procedures [22], that results in the lowest BER for each SDM

[1] It is worth noting that with the aid of powerful non-linear near Maximum Likelihood (ML) sphere decoders it is possible to separate $n_\mathrm{R} > n_\mathrm{T}$ number of layers [9].

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

Tab. 1: Investigated transmission modes

MIMO data vector. This would lead to different transmission modes per SDM MIMO data vector and a high signaling overhead would result. However, in order to avoid any signalling overhead, fixed transmission modes are used in this contribution regardless of the channel quality. The MIMO layer specific bit-error probability at the time k after SVD is given by [4]

$$P_{\mathrm{BER}}^{(\ell,k)} = \frac{2\left(1-\frac{1}{\sqrt{M_\ell}}\right)}{\log_2(M_\ell)}\,\mathrm{erfc}\left(\sqrt{\frac{\xi_{\ell,k}}{2}}\cdot\frac{U_{\mathrm{s}\,\ell}}{U_{\mathrm{R}}}\right) \quad . \tag{17}$$

The resulting average bit-error probability at time k assuming different QAM constellation sizes per activated MIMO layer results in

$$P_{\mathrm{BER}}^{(k)} = \frac{1}{\sum_{\nu=1}^{L}\log_2(M_\nu)}\sum_{\ell=1}^{L}\log_2(M_\ell)\,P_{\mathrm{BER}}^{(\ell,k)} \quad . \tag{18}$$

Taking K consecutive time slots into account, needed to transmit the SDM MIMO data vector, the aggregate bit-error probability per SDM MIMO data vector yields

$$P_{\mathrm{BER\,block}} = \frac{1}{K}\sum_{k=1}^{K}P_{\mathrm{BER}}^{(k)} \quad . \tag{19}$$

When considering time-variant channel conditions, rather than an AWGN channel, the BER can be derived by considering the different transmission block SNRs.

Assuming that the transmit power is uniformly distributed over the number of activated MIMO layers, i. e., $P_{\mathrm{s}\,\ell} = P_{\mathrm{s}}/L$, the half-level transmit amplitude $U_{\mathrm{s}\,\ell}$ per activated MIMO layer results in

$$U_{\mathrm{s}\,\ell} = \sqrt{\frac{3\,P_{\mathrm{s}}}{2\,L\,(M_\ell-1)}} \quad . \tag{20}$$

The layer-specific signal-to-noise ratio at time k, defined in (14), results together with (20) in

$$\varrho^{(\ell,k)} = \xi_{\ell,k}\,\frac{3}{2\,L\,(M_\ell-1)}\,\frac{P_{\mathrm{s}}}{U_{\mathrm{R}}^2} = \xi_{\ell,k}\,\frac{3}{L\,(M_\ell-1)}\,\frac{E_{\mathrm{s}}}{N_0} \quad , \tag{21}$$

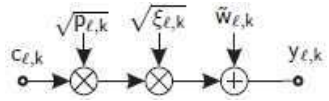

Fig. 4: *Resulting layer-specific system model including MIMO-layer PA*

with

$$\frac{P_{\mathrm{s}}}{U_{\mathrm{R}}^2} = \frac{E_{\mathrm{s}}}{N_0/2} \ . \tag{22}$$

Finally, the MIMO layer-specific BER at the time k is now given by:

$$P_{\mathrm{BER}}^{(\ell,k)} = \frac{2\left(1-\frac{1}{\sqrt{M_\ell}}\right)}{\log_2(M_\ell)} \operatorname{erfc}\left(\sqrt{\frac{3\,\xi_{\ell,k}}{2\,L\,(M_\ell-1)}\,\frac{E_{\mathrm{s}}}{N_0}}\right) \ . \tag{23}$$

The resulting average bit-error probability taking the different number of activated MIMO layer at the time k into account, is obtained as

$$P_{\mathrm{BER}}^{(k)} = \frac{2}{R}\sum_{\ell=1}^{L}\left(1-\frac{1}{\sqrt{M_\ell}}\right) \operatorname{erfc}\left(\sqrt{\frac{3\,\xi_{\ell,k}}{2\,L\,(M_\ell-1)}\,\frac{E_{\mathrm{s}}}{N_0}}\right) \ , \tag{24}$$

with

$$R = \sum_{\ell=1}^{L}\log_2(M_\ell) \ , \tag{25}$$

describing the number of transmitted bits at the time k. Finally, the aggregate bit-error probability per SDM MIMO data block can be calculated by taking (19) into account.

4 Adaptive MIMO-layer Power Allocation

In systems, where channel state information is available at the transmitter side, the knowledge about how the symbols are attenuated by the channel can be used to adapt the transmit parameters. Power allocation can be used to balance the bit-error probabilities in the activated MIMO layers. Adaptive power allocation (PA) has been widely investigated in the literature [15, 18, 12, 1].

The BER of the uncoded MIMO system is dominated by the specific layers having the lowest SNR's. As a remedy, a MIMO-layer transmit PA scheme is required for minimizing the overall BER under the constraint of a limited total MIMO transmit power. The proposed PA scheme scales the half-level transmit amplitude $U_{\mathrm{s}\,\ell}$ of the ℓth MIMO layer by the factor $\sqrt{p_{\ell,k}}$. This results in a MIMO layer-specific transmit amplitude of $U_{\mathrm{s}\,\ell}\sqrt{p_{\ell,k}}$ for the QAM symbol of

the transmit data vector transmitted at the time k over the MIMO layer ℓ (Fig. 4). Applying MIMO-layer PA, the half vertical eye opening per MIMO layer ℓ at the time k becomes

$$U_{\mathrm{PA}}^{(\ell,k)} = \sqrt{p_{\ell,k}} \cdot \sqrt{\xi_{\ell,k}} \cdot U_{\mathrm{s}\,\ell} \ . \tag{26}$$

Now the layer-specific signal-to-noise ratio, defined in (21), is changed to

$$\varrho_{\mathrm{PA}}^{(\ell,k)} = \frac{\left(U_{\mathrm{PA}}^{(\ell,k)}\right)^2}{U_{\mathrm{R}}^2} = p_{\ell,k} \cdot \frac{3\,\xi_{\ell,k}}{L\,(M_\ell - 1)} \frac{E_{\mathrm{s}}}{N_0} = p_{\ell,k} \cdot \varrho^{(\ell,k)} \ . \tag{27}$$

Using (12) and (27), along with the MIMO detector's input noise power, the resultant layer-specific BER at the time k can be calculated according to

$$P_{\mathrm{BER\,PA}}^{(\ell,k)} = \frac{2\left(1 - \frac{1}{\sqrt{M_\ell}}\right)}{\log_2(M_\ell)} \operatorname{erfc}\left(\sqrt{\frac{3\,p_{\ell,k}\,\xi_{\ell,k}}{2\,L\,(M_\ell - 1)} \frac{E_{\mathrm{s}}}{N_0}}\right) \ . \tag{28}$$

Finally, the BER at the time k, applying MIMO-layer PA, results in

$$P_{\mathrm{BER\,PA}}^{(k)} = \frac{2}{R} \sum_{\ell=1}^{L} \left(1 - \frac{1}{\sqrt{M_\ell}}\right) \operatorname{erfc}\left(\sqrt{\frac{3\,p_{\ell,k}\,\xi_{\ell,k}}{2\,L\,(M_\ell - 1)} \frac{E_{\mathrm{s}}}{N_0}}\right) \ . \tag{29}$$

The aggregate bit-error probability per SDM MIMO data block can be calculated by taking (19) into account. Applying MIMO-layer PA, the information about how the symbols are attenuated by the channel, i. e., the singular-values, has to be sent via a feedback channel to the transmitter side and leads to a high signalling overhead that is contradictory to the fix transmission modes that require no signalling overhead. However, as shown in [6] a vector quantizer (VQ) can be used to keep the signalling overhead moderate. Here, a VQ for the power allocation parameters instead of the singular values guarantees a better adaption at a given codebook size, since the power level vectors has less or equal dimensions than the singular-value vectors [6]. Moreover, its elements are much smaller digits ranged from 0 to 1, rather than from 0 to $+\infty$ in the singular-value vector case. Hence, the entropy of the power level vectors is smaller, which benefits the quantization accuracy and the feedback overhead.

The aim of the forthcoming discussions is now the determination of the values $\sqrt{p_{\ell,k}}$ for the activated MIMO layers. A common strategy is to use the Lagrange multiplier method in order to find the optimal value of $\sqrt{p_{\ell,k}}$ for each MIMO layer ℓ and time k needed to transmit the SDM MIMO data vector. The Lagrangian cost function $J(p_{1,k}, \cdots, p_{L,k})$ may be expressed with (29) as

$$J(p_{1,k}, \cdots, p_{L,k}) = P_{\mathrm{BER\,PA}}^{(k)} + \lambda\, B_L \ , \tag{30}$$

where λ is the Lagrange multiplier [18]. The parameter B_L in (30) describes the boundary condition taking the transmit power restriction per time slot into account and results in

$$B_L = \sum_{\ell=1}^{L} p_{\ell,k} - L = 0 \ . \tag{31}$$

Unfortunately, the Lagrange multiplier method often leads to excessive-complexity optimization problems [4]. Therefore, suboptimal power allocation strategies having a lower complexity are of common interest [4, 18]. A natural choice is to opt for a PA scheme, which results in an identical signal-to-noise ratio

$$\varrho_{\mathrm{PA\,equal}}^{(\ell,k)} = \frac{\left(U_{\mathrm{PA\,equal}}^{(\ell,k)}\right)^2}{U_{\mathrm{R}}^2} = p_{\ell,k} \cdot \varrho^{(\ell,k)} \tag{32}$$

for all activated MIMO layers at the time k, i. e., in

$$\varrho_{\mathrm{PA\,equal}}^{(\ell,k)} = \text{constant} \quad \ell = 1, 2, \cdots, L \ . \tag{33}$$

The power to be allocated to each activated MIMO layer at the time k can be shown to be calculated as follows [4]:

$$p_{\ell,k} = \frac{(M_\ell - 1)}{\xi_{\ell,k}} \cdot \frac{L}{\sum\limits_{\nu=1}^{L} \frac{(M_\nu - 1)}{\xi_{\nu,k}}} \ . \tag{34}$$

The only difference between the optimum PA and the equal SNR PA is the consideration of the factor $(1 - 1/\sqrt{M_\ell})$ by the optimum PA. Taking (34) and (20) into account, for each symbol of the SDM MIMO data vector, transmitted at the time k over the number of activated MIMO layers, the same half vertical eye opening of

$$U_{\mathrm{PA\,equal}}^{(\ell,k)} = \sqrt{p_{\ell,k}} \cdot \sqrt{\xi_{\ell,k}} \cdot U_{\mathrm{s}\,\ell} = \sqrt{\frac{3\,P_{\mathrm{s}}}{2\sum\limits_{\nu=1}^{L} \frac{(M_\nu - 1)}{\xi_{\nu,k}}}} \tag{35}$$

can be guaranteed ($\ell = 1, \cdots, L$), i. e.,

$$U_{\mathrm{PA\,equal}}^{(\ell,k)} = \text{constant} \qquad \ell = 1, 2, \cdots, L \ . \tag{36}$$

When assuming an identical detector input noise variance for each channel output symbol, the above-mentioned equal quality scenario (33) is encountered, i. e.,

$$\varrho_{\mathrm{PA\,equal}}^{(\ell,k)} = \frac{\left(U_{\mathrm{PA\,equal}}^{(\ell,k)}\right)^2}{U_{\mathrm{R}}^2} = \frac{E_{\mathrm{s}}}{N_0} \frac{3}{\sum\limits_{\nu=1}^{L} \frac{(M_\nu - 1)}{\xi_{\nu,k}}} \ . \tag{37}$$

Analyzing (37), nearly the same BER can be achieved on all activated MIMO layers at a given time k. However, different BERs arise for the K consecutive time slots needed to transmit a given SDM MIMO data vector. Therefore, the BER per SDM MIMO signal vector is mainly dominated by the symbol positions having the lowest SNR's. Furthermore, taking the time-variant nature of the transmission channel into account, different BERs arise for different SDM MIMO data blocks. In order to overcome this problem, the number of transmit or receive antennas has to be increased or coding over the different data blocks should be used [3, 2].

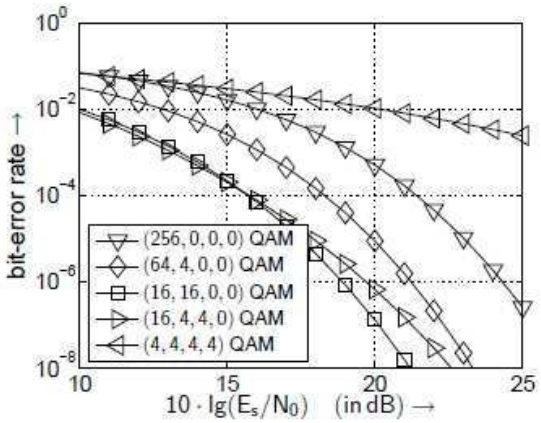

Fig. 5: *BER without PA when using the transmission modes introduced in Tab. 1 and transmitting 8 bit/s/Hz over frequency selective channels with* $L_c = 1$

5 Results

In this contribution the efficiency of fixed transmission modes is studied regardless of the channel quality. Assuming predefined transmission modes, a fixed data rate can be guaranteed. The obtained BER curves are depicted in Fig. 5 and 6 for the different QAM constellation sizes and MIMO configurations of Tab. 1, when transmitting at a bandwidth efficiency of 8 bit/s/Hz within a given bandwidth[2].

Assuming a uniform distribution of the transmit power over the number of activated MIMO layers, it turns out that not all MIMO layers have to be activated in order to achieve the best BERs. More explicitly, our goal is to find that specific combination of the QAM mode and the number of MIMO layers, which gives the best possible BER performance at a given fixed bit/s/Hz bandwidth efficiency. The E_s/N_0 value required by each scheme at BER 10^{-4} was extracted from Fig. 5 and 6 and the best systems are shown in bold in Tab. 1. Comparing the results depicted in Fig. 5 and 6, it can be seen that a high delay spread is quite beneficial for a good overall performance.

Further improvements are possible by taking the adaptive allocation of the transmit power into account. The differences between the optimal and the suboptimal equal SNR PA, as investigated in [5], show a negligible performance gap between the optimal and the equal SNR PA. The only difference between the optimum PA and the equal SNR PA is the consideration of the factor $(1-1/\sqrt{M_\ell})$ by the optimum PA. However, their influence, introduced by the layer-specific QAM constellation sizes, is by far too small to generate remarkable differences in the

[2]The expression $\lg(\cdot)$ is considered to be the short form of $\log_{10}(\cdot)$.

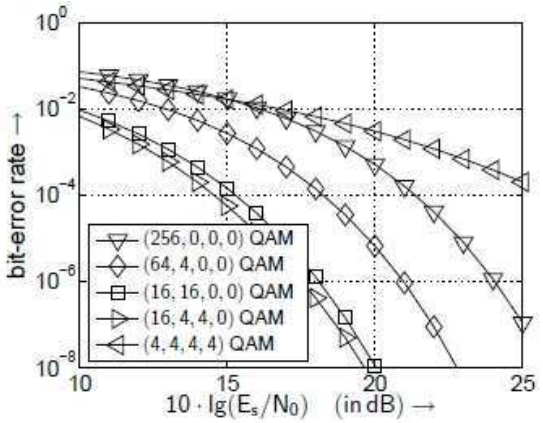

Fig. 6: *BER without PA when using the transmission modes introduced in Tab. 1 and transmitting* 8 *bit/s/Hz over frequency selective channels with* $L_c = 4$

performance [5]. Furthermore, from Fig. 7 and 8 we see that unequal PA is only effective in conjunction with the optimum number of MIMO layers. Using all MIMO layers, our PA scheme would assign much of the total transmit power to the specific symbol positions per MIMO layer having the smallest singular values and hence the overall performance would deteriorate.

mode	$(16, 4, 4, 0)$	$(16, 16, 0, 0)$	$(64, 4, 0, 0)$	$(4, 4, 4, 4)$
pdf	0.881	0.112	0.007	0

Tab. 2: Probability of choosing specific transmission modes at a fixed data rate by using optimal bitloading ($10 \cdot \mathsf{lg}(E_s/N_0) = 10$ dB and $L_c = 1$)

However, the lowest BERs can only be achieved by using bit auction procedures leading to a high signalling overhead [22]. Analyzing the probability of choosing a specific transmission mode by using optimal bitloading, as depicted in Tab. 2, it turns out that only an appropriate number of MIMO layers has to be activated, e. g., the $(16, 4, 4, 0)$ QAM configurations. The results, obtained by using bit auction procedures justify the the choice of fixed transmission modes regardless of the channel quality as investigated in the contribution.

6 Conclusion

Bit and power loading in broadband MIMO systems were investigated. It turned out, that the choice of the number of bits per symbol as well as the number of

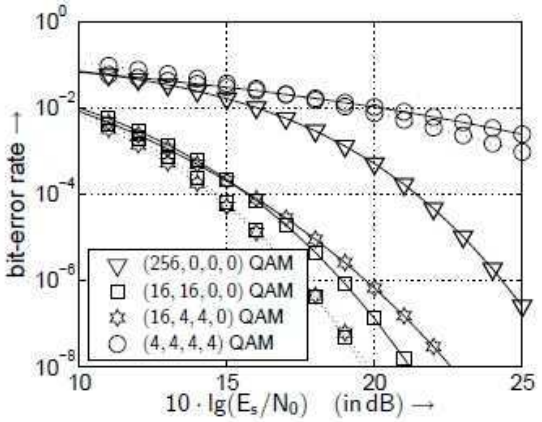

Fig. 7: *BER with PA (dotted line) and without PA (solid line) when using the transmission modes introduced in Tab. 1 and transmitting* 8 *bit/s/Hz over frequency selective channels with* $L_c = 1$

activated MIMO layer substantially affects the performance of a MIMO system, suggesting that not all MIMO layers have to be activated in order to achieve the best BERs. The main goal was to find that specific combination of the QAM mode and the number of MIMO layers, which gives the best possible BER performance at a given fixed bit/s/Hz bandwidth efficiency. The E_s/N_0 value required by each scheme at BER 10^{-4} was extracted from computer simulations and the best systems are shown in bold in Tab. 1.

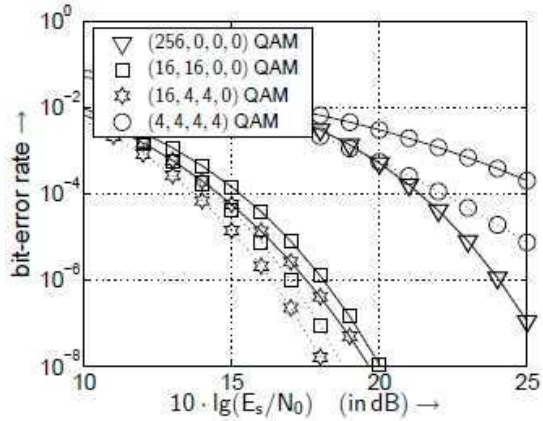

Fig. 8: *BER with PA (dotted line) and without PA (solid line) when using the transmission modes introduced in Tab. 1 and transmitting* 8 *bit/s/Hz over frequency selective channels with* $L_c = 4$

References

[1] A. Ahrens and C. Benavente-Peces. Modulation-Mode and Power Assignment in SVD-assisted Broadband MIMO Systems. In *International Conference on Wireless Information Networks and Systems (WINSYS)*, pages 83–88, Milan (Italy), 06.–10. July 2009.

[2] A. Ahrens and V. Kühn. Modulation-Mode and Power Assignment for MIMO-BICM Schemes. In *IEEE International Workshop on Smart Antennas (WSA)*, pages 262–269, Darmstadt, 26.–27. February 2008.

[3] A. Ahrens, V. Kühn, and T. Weber. Iterative Detection for Spatial Multiplexing with Adaptive Power Allocation. In *7th International Conference on Source and Channel Coding (SCC)*, Ulm, January 2008.

[4] A. Ahrens and C. Lange. Transmit Power Allocation in SVD Equalized Multicarrier Systems. *International Journal of Electronics and Communications (AEÜ)*, 61(1):51–61, 2007.

[5] 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.

[6] A. Ahrens and C. Lange. Modulation-Mode and Power Assignment in SVD-assisted MIMO Systems with limited Feedback. In *First Asian Conference on e-Business and Telecommunications (CeBT)*, pages 1–18, Changhua City (Taiwan), 09.–10. February 2009.

[7] G. D. Forney, R. G. Gallager, G. R. Lang, F. M. Longstaff, and S. U. Qureshi. Efficient Modulation for Band-Limited Channels. *IEEE Journal on Selected Areas in Communications*, 2(5):632–647, 1984.

[8] D. Gesbert. Multipath: Curse or Blessing? A System Performance Analysis of MIMO Wireless Systems. In *Proceedings of International Zurich Seminar on Communications (IZS)*, pages 14–17, Zurich (Switzerland), 2004.

[9] L. Hanzo and T. Keller. *OFDM and MC-CDMA.* Wiley, New York, 2006.

[10] S. S. Haykin. *Adaptive Filter Theory.* Prentice Hall, New Jersey, 2002.

[11] F.-M. Hsu. Data Directed Estimation Techniques for Single-Tone HF Modems. In *IEEE Military Communications Conference (MILCOM)*, pages 271–280, 1985.

[12] T. Hunziker and D. Dahlhaus. Optimal Power Adaptation for OFDM Systems with Ideal Bit-Interleaving and Hard-Decision Decoding. In *IEEE International Conference on Communications (ICC)*, volume 1, pages 3392–3397, Anchorage, Alaska (USA), May 2003.

[13] I. Kalet. Optimization of Linearly Equalized QAM. *IEEE Transactions on Communications*, 35(11):1234–1236, November 1987.

[14] I. Kalet. The Multitone Channel. *IEEE Transactions on Communications*, 37(2):119–124, Februar 1989.

[15] B. S. Krongold, K. Ramchandran, and D. L. Jones. Computationally Efficient Optimal Power Allocation Algorithms for Multicarrier Communications Systems. *IEEE Transactions on Communications*, 48(1):23–27, 2000.

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

[17] N. Palleit, A. Ahrens, and C. Lange. Transmit Power Allocation in SVD-equalized Broadband MIMO Transmission Systems. In *International Conference on Advances in the Internet, Processing, Systems, and Interdisciplinary Research (IPSI)*, New York (USA), 05.–08. Januar 2006.

[18] C. S. Park and K. B. Lee. Transmit Power Allocation for BER Performance Improvement in Multicarrier Systems. *IEEE Transactions on Communications*, 52(10):1658–1663, 2004.

[19] J. G. Proakis. *Digital Communications.* McGraw-Hill, Boston, 2000.

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

[21] 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.

[22] C. Y. Wong, R. S. Cheng, K. B. Letaief, and R. D. Murch. Multiuser OFDM with Adaptive Subcarrier, Bit, and Power Allocation. *IEEE Journal on Selected Areas in Communications*, 17(10):1747–1758, October 1999.

[23] L. Zheng and D. N. T. Tse. Diversity and Multiplexing: A Fundamental Tradeoff in Multiple-Antenna Channels. *IEEE Transactions on Information Theory*, 49(5):1073–1096, May 2003.

[24] Z. Zhou, B. Vucetic, M. Dohler, and Y. Li. MIMO Systems with Adaptive Modulation. *IEEE Transactions on Vehicular Technology*, 54(5):1073–1096, September 2005.

Strategies for Resource Management in Wireless Sensor Networks

Jiaxi You, Dirk Timmermann
Institute of Applied Microelectronics and Computer Engineering
University of Rostock, 18119 Rostock, Germany
Email: jiaxi.you@uni-rostock.de

Abstract

Along with the emergence of Wireless Sensor Network (WSN) applications, energy efficiency, Quality-of-Service (QoS) and scalability are becoming key design challenges. In our former work, various clustering and routing algorithms have been proposed as management strategies for WSNs. In this paper, we classify WSNs according to their properties of deployment, and summarize our management strategies to address the characteristics of each class. We mainly focus on the clustering and routing algorithms, where various kinds of context information are utilized as design parameters to achieve optimal performance.

1 Introduction

Wireless Sensor Networks (WSNs) are composed of sensor nodes, which measure physical parameters in terrains of interest, such as temperature, humidity, presence of objects etc., and send gathered data to a data sink where information is processed. As sensor nodes are left unattended after deployment, sensor nodes are usually battery powered. Therefore, energy remains one of the critical resources of WSNs. One of the main components of energy consumption is wireless communication that is usually carried out by on-board radio transceivers. During radio signal propagation, the transmission power decreases proportionally to the square of distance or worse. For nodes with limited transmission power, transmission range as well as bandwidth is also highly constrained in WSNs. Recent advances of electronic technology yield small and inexpensive sensor nodes [6], and motivate development of large-scale networks. Therefore, scalability is becoming another major design attribute of WSNs.

Since radio communication among sensor nodes is the main drain of energy in WSNs, reducing the amount of radio transmission becomes the goal of our resource management. Clustering and routing algorithms are two major research fields to address the objectives (e.g. prolonging the lifetime of WSNs, achieving scalability for large-scale networks, etc.) of our management strategies. The objective is the efficient use of resources (e.g. battery power, bandwidth, etc.) in WSNs.

2 Strategies of Resource Management

Management of WSNs can be either centralized or distributed. In a centralized WSN, nodes are connected hierarchically with the data sink as the root of the structure [15, 11]. In contrast, networks of large physical dimension tend to be distributed, meaning that nodes are organized locally and communicate with each other using multi-hop routing. [9, 13].

By organizing nodes into small groups, clustering techniques aid effectively to the energy-efficiency and scalability of large-scale WSNs. A generic cluster has a cluster head and several cluster members. Sensor nodes transmit data only to the local cluster heads which aggregate received data and route them to data sink. Aggregated data is routed to data sink through an overlay of cluster heads [16], while releasing the cluster members from the global routing tasks.

In centralized networks, routing paths are established statically using specific network structures. In [15] and [11], a WSN is structured as a spanning tree joint by cluster heads, with the data sink at its root. In distributed networks, routing paths are built dynamically using the local knowledge of nodes [14, 10, 12]. For delay sensitive WSN applications that require real-time services, time for a detected event to arrive at data sink is of significant importance. In WSNs, efficient routing paths between sensor nodes and data sink can help to achieve both energy-conservation and high QoS.

In [11, 14, 10, 12, 13], we have proposed various clustering and routing algorithms as management strategies for WSNs. In this paper, we categorize WSNs according to their properties, and apply our algorithms to suit each class. The taxonomy of our strategies is illustrated in Figure 1. Our algorithms tightly involve context information as important parameters. For instance, the battery status of sensors is one of the essential considerations during clustering and routing processes. As WSNs are deployed to various environments, context information regarding the terrain can influence the performance of WSNs. The existence of deployment voids, for example, is also considered as an important parameter of designing the clustering and routing algorithms.

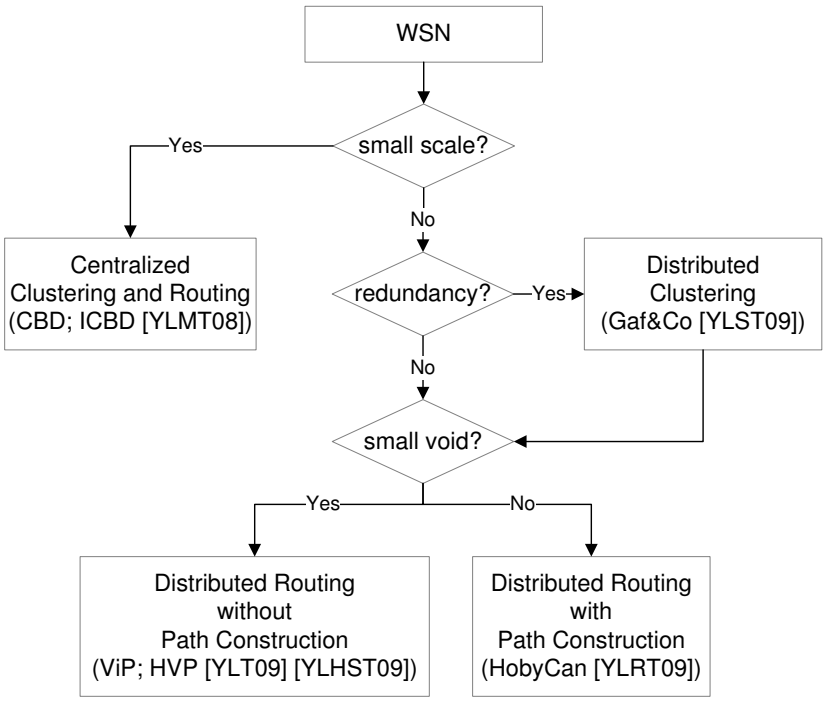

Fig. 1: *Classification of WSNs and management strategies*

2.1 Strategies in centralized WSNs

Small-scale WSNs are usually organized in a centralized manner, where nodes are connected in a static structure to the data sink. We proposed the Clustering with Dynamic Budget (CDB) algorithm and the Interactive Clustering with Dynamic Budget (ICDB) algorithm [11] to generate spanning tree structures (Figure 2(a)) in WSNs, where hierarchical routing from nodes to data sink can be applied. Both clustering algorithms do not only target energy conservation and scalability of WSNs, but also efficient routing between sensor nodes and data sink. CDB and ICDB initiate a clustering process from the data sink, and recruit nodes in the growing tree structure.

Careful selection of cluster heads and optimal formation of clusters help to improve the end-to-end delay of packets. Clusters with bounded sizes contribute dramatically to the efficient task allocation and energy balance within WSNs [5]. A way to form bounded clusters is to constrain cluster sizes with a predefined budget value. In such budget-based clustering algorithms, cluster heads are assigned budget values that indicate the maximum number of their cluster members. Sensor nodes in a network typically have different remaining energy or activities, which contributes to the complexity of the network. Our algo-

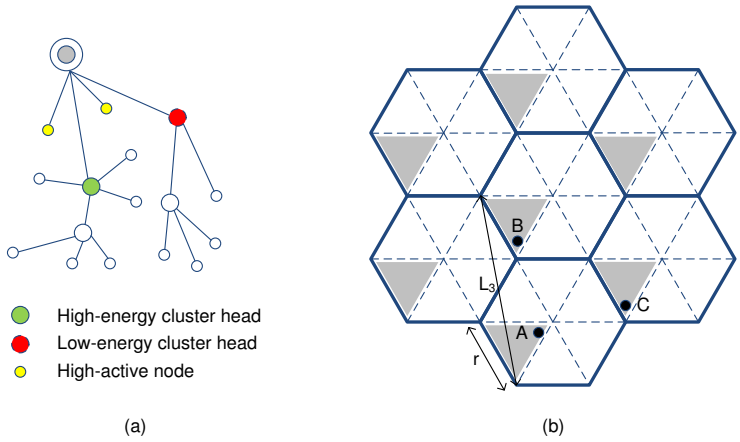

Fig. 2: *Classification of WSNs and clustering strategies. (a). Centralized hierarchical clustering (CDB; ICDB). (b). Distributed geographic clustering (GAF&Co).*

rithms utilize such context information in estimation of dynamic budget values, election of cluster heads, as well as selection of cluster members. In CDB, cluster heads with more remaining energy are assigned bigger budget values to improve load balancing. Sensor nodes with higher activity rates are placed nearer (in terms of hops in a spanning tree) to data sink, so fewer hops will be needed for frequent messages coming from the active nodes. As an extension to CDB, ICDB employs activity rates of cluster members as feedback to further optimize the size of the clusters.

2.2 Strategies in distributed WSNs

Large-scale WSNs tend to be organized in a distributed manner, where nodes are locally self-organized. Routing via multiple hops is the major source of energy consumption in distributed WSNs, which also affects significantly QoS of the network application. Among various routing algorithms, single-path geographic routing with Greedy Forwarding (GF) is attractive for WSNs [2]. In a basic GF algorithm, a node communicates only with its direct neighbors (1-hop). The neighboring node that further minimizes the remaining distance of a packet to its destination is selected as the next hop. Such localized routing approach is effective and accommodates dynamically to changes, which only requires position information of sensor nodes.

However, voids in the deployment or node failure can cause routing holes [1] in the network, which often cause traditional geographic routing algorithms to fail. This is basically caused by the local minimum phenomenon illustrated in

Figure 3(a). When using GF, packets get stuck at node A since there is no neighbor node closer to the destination than node A itself. In this section, we summarize our strategies addressing the local minimum problem from different perspectives. In dense networks, distributed clustering algorithm GAF&Co [13] is used to conserve energy by switching off redundant nodes. For carefully deployed networks, simple variants of GF (VIP; HVP [14, 10]) are introduced to bypass small routing holes while keeping overhead low. For networks with large voids, dedicated detour paths are constructed with routing algorithm HobyCan [12] around routing holes.

Distributed geographic clustering (GAF&Co): As more and more sensor nodes are employed in modern WSNs, redundancy of sensor nodes can be utilized to conserve energy. Some clustering algorithms [9, 7] divide a geographical region into a number of smaller zones, namely clusters. Nodes are classified into clusters according to their geographic properties. In each cluster, only one representative node is active, while the redundant nodes operate in energy-saving mode to prolong network lifetime. Routing activities are carried out only by the representative nodes, namely the cluster heads.

It is observed that the connectivity of a network is reduced by such clustering algorithms, where only a subset of nodes is involved in global routing. When applying a generic geographic routing algorithm, it is more likely to encounter the routing hole problem as only a subset of nodes is active. We presented a novel clustering algorithm called GAF with COnnectivity-awareness (GAF&Co) to prevent routing holes introduced by switching off nodes. The proposed algorithm divides a network into hierarchical hexagonal cells, as in Figure 2(b). Each hexagonal cell has 6 triangular sub-cells. One set of the sub-cells with the same relative position in the hexagonal cells are set to be the active sub-cells, where one sensor node of each sub-cell is kept active for routing activities. The rest of sensor nodes are switched to energy-saving mode.

The main objective of GAF&Co is to avoid routing holes caused by existing clustering strategies. As in Figure 3(b), the maximal angle formed by points in an active sub-cell and its 2 neighboring active sub-cells (angular adjacent) is not greater than $2\pi/3$. As proved in the TENT rule [3], a node is not a local minimum when there is no angle spanned by a pair of its angularly adjacent neighbors greater than $2\pi/3$. In GAF&Co, as long as every sub-cell has at least one sensor node, local minimums can be eliminated and geographic routing with greedy forwarding can be simply applied.

Look-ahead geographic routing for smaller voids (ViP; HVP): Many ideas have been proposed to address the routing hole problem in WSNs [1]. To improve the success rate of geographic routing for sparsely-deployed WSNs

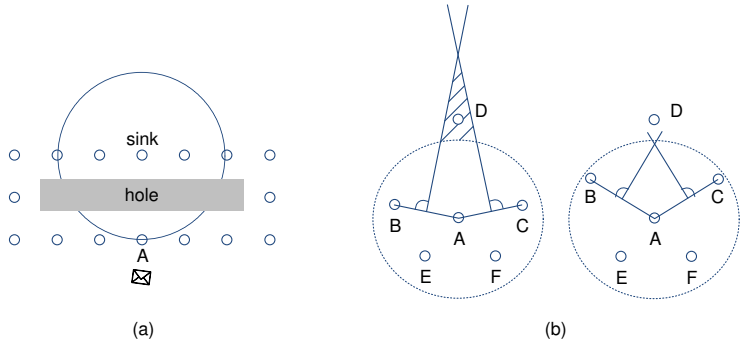

Fig. 3: *(a). An example of local minimum (node A). (b). An example of TENT rule. When $\angle$ BAC is greater than $2\pi/3$ (left figure), the perpendicular bisector of BA and CA, together with the communication bounder of node A, forms a shadowed area outside the transmission range of node A, where a point is closer to node A than to node B or node C. When a packet with a destination (e.g. node D) in the shadowed area arrives, node A becomes a local minimum since there is no neighbor closer to the destination than node A itself. When the minimal angle formed by 2 angular adjacent neighbors of node A is not greater than $2\pi/3$ (right figure), the shadowed area disappears and node A can always find a neighbor which is nearer to any point outside its transmission range.*

or WSNs with small routing holes, we proposed the Greedy Forwarding with Virtual Position (ViP) and the Greedy Forwarding with Hierarchical Virtual Position (HVP) algorithms [14, 10]. The main advantage of our approaches is that the algorithms simply employ GF throughout the routing process, and inherently result in high routing efficiency as the basic GF algorithms. In the mean time, the amount of control overhead of the proposed algorithms is strictly limited.

The *virtual position* of a node is introduced as the middle point of all its direct neighbors. Each node calculates its virtual position, and broadcasts its virtual position to its direct neighbors. The information of virtual position is stored on nodes themselves and their direct neighbors. The virtual position of a node indicates how the direct neighbors are located around the node on average, hence it is a suitable metric to demonstrate the tendency of further forwarding during geographic routing.

ViP is a look-ahead geographic routing algorithm based on the coordinate system of virtual positions. ViP uses virtual positions of nodes to consider farther neighbors in the look-ahead routing process, and therefore avoids packets from going into local minimums. ViP has two variants called Greedy-ViP and MFR-ViP, which are based on the principle of the two basic GF algorithms, the Greedy [4] and MFR (Most Forwarding progress within Radius) [8], respectively. An example of ViP is shown in Figure 4(a). To further improve the success rate,

we extended ViP to "higher-level virtual position" that considers farther nodes (neighbors of K-Hop, K≥1) in routing. The K^{th}-level virtual position (K≥2) of a node can be iterated from the $(K-1)^{th}$-level virtual positions of the node and its direct neighbors. We also proposed HVP to use the combination of all K-level virtual positions (K≥1) and the geographic positions of nodes.

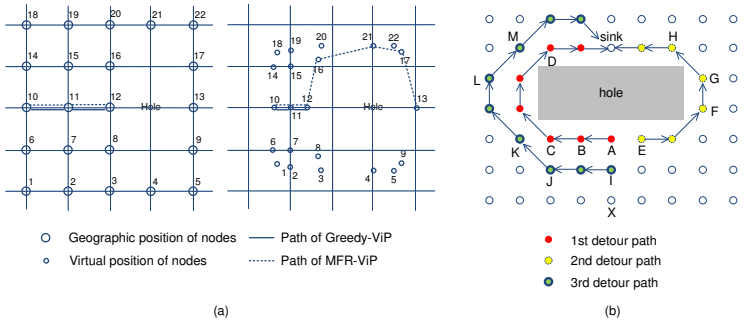

Fig. 4: *Classification of distributed WSNs and routing strategies (a). An example of the ViP algorithm. For a packet from node 10 to node 13, both Greedy and MFR get stuck at node 12, since there is no neighbor that can make further progress towards the destination. In contrast, the virtual position of node 12 is strongly left-biased due to the void on the right side of node 12. As a result, MFR-ViP finds a path (10-11-12-16-21-17-13) around the hole using virtual positions of nodes. (b). An example of the HobyCan algorithm, where 3 detour paths are constructed around a routing hole.*

Routing path construction for large voids (HobyCan): To lead packets around large routing holes, we proposed a novel geographic routing algorithm "HOle-BYpassing routing with Context-AwareNess (HobyCan)" [12]. Our algorithm dynamically constructs multiple detour paths around routing hole(s) and uses them alternatively for routing.

HobyCan protocol is designed for the common "many-to-one" communication model of WSNs, where packets are sent from sensor nodes towards a single data sink. Therefore, detour paths are constructed from a local minimum up to the data sink. As in Figure 4(b), detour paths are disjoint from each other, while packets can be transferred from one detour path to another based on the context of the network. For packet routing around a hole, a suitable path can be dynamically determined from the set of detour paths. As a result, the energy consumption is fairly distributed with more nodes on extra detour paths. Such mechanism aims at finding optimal routing paths, as well as balancing of routing load among sensor nodes.

3 Conclusion

In this paper, we analyze the properties of WSNs from the system perspective, and classify them into different categories. In order to manage the resources (e.g. battery power, bandwidth, etc.) in WSNs, we review the clustering and routing algorithms in our former work, and apply them to meet the characteristic of WSNs of each category. The objectives of our management strategies are prolonging the lifetime of WSNs, meeting the QoS, and achieving scalability for large-scale networks.

References

[1] Nadeem Ahmed, Salil S. Kanhere, and Sanjay Jha. The holes problem in wireless sensor networks: a survey. ACM SIGMOBILE Mobile Computing and Communi-cations Review, v.9 n.2, April 2005.

[2] K. Akkaya and M. Younis. A survey of routing protocols for wireless sensor networks. *Elsevier Ad Hoc Network Journal*, 3/3:325–349, 2005.

[3] Qing Fang, Jie Gao, and Leonidas J. Guibas. Locating and bypassing routing holes in sensor networks. In IEEE INFOCOM 2004, June 2004.

[4] G. G. Finn. Routing and addressing problems in large metropolitan-scale internetworks. Technical Report ISI/RR-87-180, Information Sciences Institute, Mars 1987.

[5] R. Krishnan and D. Starobinski. Efficient clustering algorithms for self-organizing wireless sensor networks. In *Ad Hoc Networks*, volume 4, pages 36–59, January 2006.

[6] G. J. Pottie and W. J. Kaiser. Wireless Integrated Network Sensors. In *Communications of the ACM*, volume 43, pages 51–58, May 2000.

[7] J. Salzmann, S. Kubisch, F. Reichenbach, and D. Timmermann. Energy and Coverage Aware Routing Algorithm in Self Organized Sensor Networks. 4th International Conference on Networked Sensing Systems, Braunschweig, Germany, 2007.

[8] H. Takagi and L. Kleinrock. Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals. 32(3):246–257, 1984.

[9] Y. Xu, J. Heidemann, and D. Estrin. Geography-informed energy conservation for ad hoc routing. 7th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom 01), Rome, Italy, July 2001.

[10] J. You, D. Lieckfeldt, Q. Han, J. Salzmann, and D. Timmermann. Look-ahead Geographic Routing for Sensor Networks. 5th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing (IEEE PerSeNS2009), Galveston, Texas, USA, March 9-13, 2009.

[11] J. You, D. Lieckfeldt, M. Handy, and D. Timmermann. Budget-Based Clustering with Context-awareness for Sensor Networks. 4th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing (IEEE PerSeNS2008), Hong Kong, China, March 2008.

[12] J. You, D. Lieckfeldt, F. Reichenbach, and D. Timmermann. Context-aware Geographic Routing for Sensor Networks with Routing Holes. IEEE Wireless Communications and Networking Conference (IEEE WCNC2009), Budapest, Hungary, April 5-8, 2009.

[13] J. You, D. Lieckfeldt, J. Salzmann, and D. Timmermann. GAF&Co: Connectivity Aware Topology Management for Sensor Networks. 20th IEE International Symposium on Personal, Indoor and Mobile Radio Communications, Tokyo, Japan, 2009.

[14] J. You, D. Lieckfeldt, and D. Timmermann. Tendency-based Geographic Routing for Sensor Networks. 6th Annual IEEE Consumer Communications & Networking Conference (IEEE CCNC2009), Las Vegas, USA, January 2009.

[15] M. Younis, M. Youssef, and K. Arisha. Energy-aware routing in cluster-based sensor network. In *Proc. of MASCOTS*, October 2002.

[16] O. Younis and S. Fahmy. Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach. In *Proc. of INFOCOM*, March 2004.

Selection of Node Locations and its Effect in Co-Operative ARQ Protocol

Shubhabrata Roy
Center of Excellence for Information Communication and Perception Engineering
Scuola Superiore Sant' Anna
Area Della Ricerca CNR, Via Moruzzi, 1
56124 Pisa
shubhabrata.roy@sssup.it

Abstract

Cooperative ARQ (C-ARQ) is a perfect example of cooperative mechanism that increases network reliability using spatial diversity. There has been a huge interest in research community on this protocol since it enables the nodes to virtually increase their capability in terms of both communication and signal processing. Since C-ARQ mainly makes profit out of spatial diversity of the nodes it is highly important to determine the position of the nodes in order to get optimal solution. In this paper an attempt has been made to find out the node positions for optimal QoS as well as a study has been made on the performance of the system depending on nodal positions with respect to Hybrid ARQ (H-ARQ).

1 Introduction

Wireless networks are believed to capture the telecommunication market in near future because of the widespread solutions provided by them. It has experienced an exponential growth [3] in the last decade and has become critical part of daily life. Because of it's widespread acceptibility a significant number of researches have been carried out in this field and still research is going on some sectors, viz. Wireless sensor network, Ad-hoc mobile in disaster management, Swarm intelligence in wireless newtwork, Self-organizing wireless network, Wireless local area network (WLAN).

One of the most important properties of wireless medium is its broadcasting nature. Due to this some unintended recipients in the vicinities can interrupt the signal. Interference is also the result of this property only. Since data packets traverse through unguided media in case of wireless networks, many reasons like path loss, and obstacles in the path deteriorates the quality of the signal in recipient site. Automatic repeat request protocol (ARQ) had been proposed to increase data transfer reliability only. Some popular ARQ mechanisms are Stop and wait ARQ, Go-back N ARQ, and Hybrid ARQ (H-ARQ). However none of them uses the spatial diversity and eavesdropping that are two basic properties of radio medium. In cooperative ARQ (C-ARQ) these properties have been utilized along with the retransmission of the original version of the corrupted packet.

Cooperative ARQ helps to retransmit the corrupted packet by actively involving some nodes other than the source or destination that falls within the vicinity. Apart from the sender / transmitter (BS/Access point) and receiver that node is termed as relay node or the co-operator [5]. Whenever the receiver doesn't satisfactorily receive data packets the relay node is asked to transmit it to the receiver and thus enhances the channel performance. Since both channels are independent of each other thus the overall performance can be said to increase by using the spatial diversity.

However a number of researches have already been carried out on this particular domain. In this paper a delay model of a single-source single-relay cooperative ARQ protocol has been adopted [1]. This protocol is based on slotted radio networks with Poisson frame arrivals. Other work on this topic is cooperative communication in Gaussian Relay for a single source [2] and recently some works have been done on multiple sources [4, 9] also. However none of them has treated spatial design properly.

2 Working principle of a type I H-ARQ and C-ARQ Model

Throughout this paper, analysis has been carried out on type - I C-ARQ model, so the following section deals with the description of that model only. Additionally a brief description of type I H-ARQ has also been incorporated for better understanding.

In type - I H-ARQ models both error detection and correction capabilities are present. It works as follows:

Transmitter sends data frame X = I, now three cases might be possible. If I is received and decoded properly at receiver, R sends back an acknowledgement signal I+1, after which T again sends a new data frame. If I is received but not decoded properly acknowledgement I is sent requesting T to retransmit frame I. If the data frame is not received at all a timeout is used at T for retransmitting the data.

In type - I C-ARQ protocol C transmits the exact copy of the data that it received from the transmitter T. Four sequences to data and acknowledgement exchanges are possible which are described as follows:

R receives the signal properly sent by T. Here X = I is transmitted by T and acknowledged by R with a signal I+1. After acknowledgement T may transmit I+1.

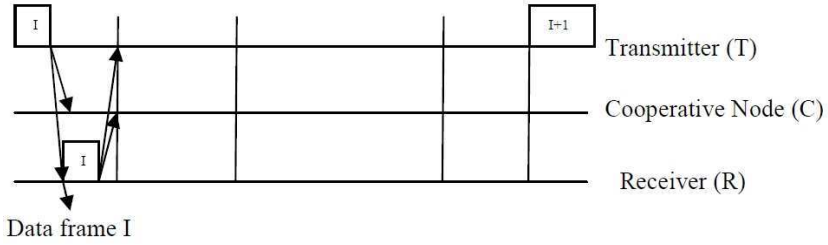

Fig. 1: *R successfully decodes the data sent by T*

In the 2nd case R receives data properly with the help of C. Data frame X = I was sent by T, which was not correctly decoded by R. But it was properly received and decoded by C. R sends a retransmission request to C using the acknowledgement signal I. After that C sends data frame I, which is correctly received by R. R sends signal I+1 to T. Next T may start to transmit X = I+1.

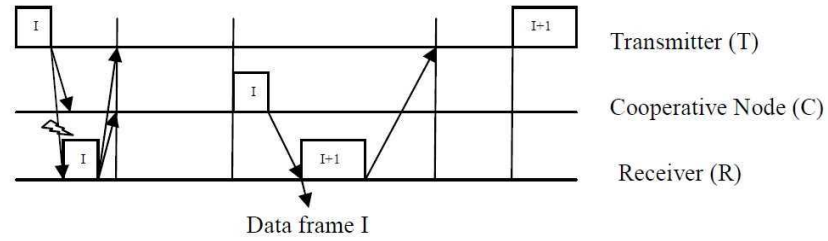

Fig. 2: *R successfully decodes data frame I with help of C*

In the 3rd case R doesn't receive data frame sent by C properly due to some transmission errors. This case starts just like the previous one; but in this case X = I, sent by C is not correctly received by R. R send signal I to T in order to request to begin a new transmission of X = I.

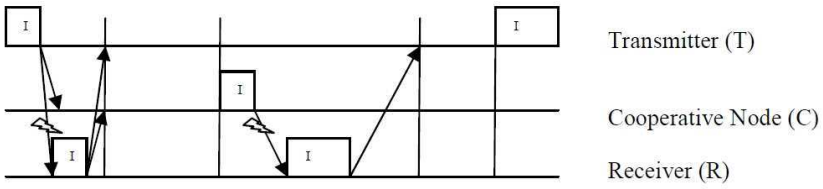

Fig. 3: *R couldn't successfully decodes data frame I sent by C because of transmission errors*

In the last case timeout gets expired. For various causes T may not get acknowledgement signal from R. Here a timeout is used to bypass deadlock. In the following figure X = I is transmitted by T, which is not correctly decoded at R. R send a retransmission request to C by signal I. But in this case even C was not able to decode the data X = I, transmitted by T. So it is not able to cooperate. Here the timeout becomes handy and upon its expiration T starts the transmission sequence X = I.

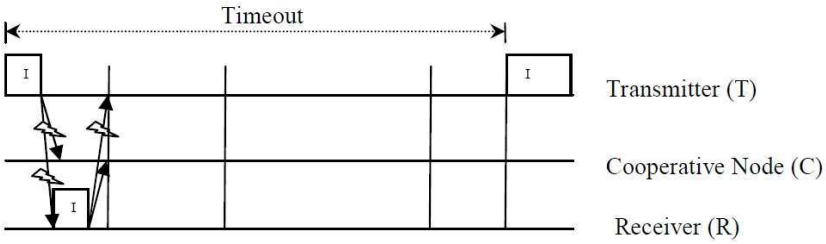

Fig. 4: *Deadlock avoidance by timeout*

3 Spatial Diversity Optimization

In this part lies the main contribution of this paper. In order to design the model following assumptions has been made:

1. The system is single source single relay single receiver model,
2. The system enjoys BPSK modulation in its physical layer,
3. All nodes have been considered identical i.e. their antenna gains are same,
4. Carrier frequency is constant throughout this protocol modelling,
5. Transmitter power is constant and doesn't vary with time,
6. Service examples implementations

7. Thermal and interference noise power doesn't vary during the operation.

With following assumptions we can consider the following equation [6]:

$$E_r = K/r^2, \tag{1}$$

where K is a constant, having a unit of $power/distance^2$ and E_r is the received power at the receiver.

In figure 2, T is the transmitter node, R is the receiver and C the cooperative or relay node.

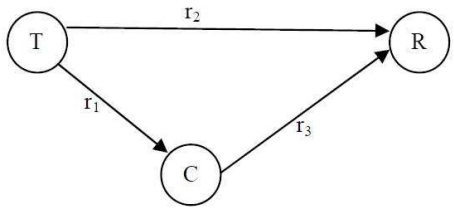

Fig. 5: *Node placement of the C-ARQ model*

Now SNR of a link (T-C or C-R etc) can be derived using [8] as follows:

$$SNR_{link} = P_r \ / \ (P_{thermal} + P_{INI}) \tag{2}$$

For $BPSK, BER_{link} = Q(\sqrt{2}\ SNR_{link})$ [8] and after proper simplification:

$$BER = Q(K_i/r) \tag{3}$$

The value of K_i depends on the value of K and thermal and interference (nodal) noise power and has been considered constant throughout this discussion.

As per the definition of Q(.) it can also be expressed approximately in terms of exponential function:

$$Q(x) = exp(-x^2/2) \ / \ (\sqrt{2}\pi)\ x \tag{4}$$

Using equation (3) for the model, described in Fig. 5, the Probability of success of getting a symbol correctly is:

$$P_{receiver} = 2 - Q(K_i/r_1) - Q(K_i/r_2) - Q(K_i/r_3) + Q(K_i/r_1)Q(K_i/r_3) \quad (5)$$

From (4) and (5),

$$\begin{aligned} P_{receiver} = 2 \ - \ \frac{exp(-K_i^2/2r_2^2)}{(\sqrt{2}\pi)K_i/r_2} \ - \ \frac{1}{(\sqrt{2}\pi)K_i}(r_1 \ exp(-K_i^2/2r_1^2) + \\ r_3 \ exp(-K_i^2/2r_3^2)) \ + \ \frac{r_1 r_3}{2\pi K_i^2} exp(-K_i^2/2)(1/2r_1^2 + 1/2r_3^2) \end{aligned} \quad (6)$$

If the distance between the transmitter and the receiver remains constant, then the entire design issue comes on the placement of the cooperative node. In this model r_2 is fixed and only variables are r_1 and r_3. So equation (6) can be written as:

$$P_{receiver} = [A - B/(\sqrt{2}\pi)K_i] \quad (7)$$

In equation (7) A is constant and only variable is B. In order to maximize the value of $P_{receiver}$ we must decrease B.

B is a function of two variables r_1 and r_3, and it can be written as:

$$\begin{aligned} B = f(r_1, r_3) = r_1 \ + \ r_3 \ + \ K_i^4(1/8r_1^3 + 1/8r_3^3) \ + \ K_i(r_1/r_3 + r_3/r_1) + \\ \frac{K_i^3}{8\sqrt{2}\pi}(r_1/r_3^3 + r_3/r_1^3) \ - \ K_i^2(1/2r_1 + 1/2r_2) \ - \ r_1 r_3/(\sqrt{2}\pi)K_i \end{aligned} \quad (8)$$

Considering $r_1 = r_1^c$ and $r_3 = r_3^c$ as the optimal points, i.e. r_1^c and r_3^c are the distance values for maximum probability of success, local minima can be guessed from equation (8) applying the below mentioned formula of 2^{nd} order partial derivative for two variables. Thus the best value for $P_{receiver}$ can be calculated.

$$D(r_1^c, r_3^c) = F_{r1r1}(r_1^c, r_3^c)F_{r3r3}(r_1^c, r_3^c) \ - \ [F_{r1r3}(r_1^c, r_3^c)]^2 > 0$$

and

$$F_{r1r1}(r_1^c, r_3^c) > 0 \quad (9)$$

Equation (9) determines the optimal distance in type I C-ARQ.

4 Effect of nodal position on performance characteristics

Queuing model of a type - I C- ARQ can be realised in terms of probability as the following figure:

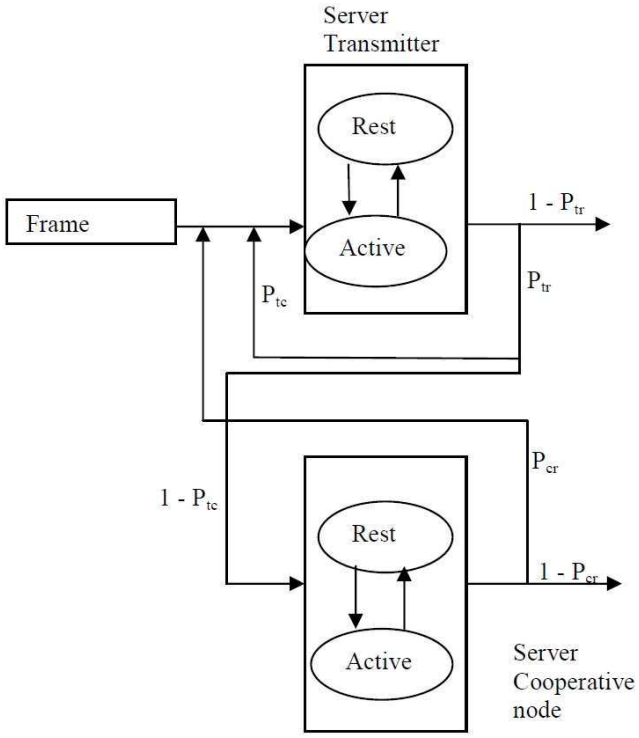

Fig. 6: *Queuing model of a type - I C-ARQ*

From [1] it can be found that if P_{tr} is the expected probability that node r doesn't successfully decode the symbol received from node t, P_{cr} is the expected probability that node r doesn't successfully decode the symbol received from node c and P_{tc} is the expected probability that node c doesn't successfully decode the symbol received from node t then the probability that upon completion of service at t the job will come back to it again (irrespective of the possibility of transition through c) can be written as:

$$P = P_{tr}(P_{tc} \ + \ (1 - P_{tc}) \ P_{cr}) \tag{10}$$

Considering P_{tr} as the corresponding probability for normal Hybrid ARQ (H-ARQ) it is possible to calculate the retransmission rate gain [1] as:

$$G_p = P(type\ I\ H-ARQ)\ /\ P(type\ I\ C-ARQ) \tag{11}$$

and throughput gain [1] as

$$G_{th} = [1\ -\ P(type\ I\ C-ARQ)]\ /\ [1\ -\ P(type\ I\ H-ARQ)] \tag{12}$$

Since for BPSK bit error rate and symbol error rate are equal [7] we can use equations (3) and (5) in order to check the effect of the nodal position on the performance index.

5 Results

In order to analyze the C-ARQ model the above mentioned performance indices retransmission gain (G_p) and throughput gain (G_{th}) have been considered. Variations of these two parameters have been studied with respect to the change in the distance (r_3) between co-operative node and the receiver node. Here the distance (r_2) between the transmitter and the receiver has been considered fixed and sum of the distances between the transmitter and the relay (r_1) and the relay and the receiver (r_3) have been considered fixed for each analysis. Thus it is possible to analyze the variation of the gains with respect to r_3 considering some fixed predefined values of $r_1 + r_3$.

In this curve change of value in G_p has been shown with respect to the change in r_3 considering some appropriate values of K_i, r_2 and $r_1 + r_3$.

6 Conclusions

From the curve it is possible to do comparative analysis of the effect of node placement on different performance index. It is clear that the distance between the relay and the receiver should be kept as low as possible in order to maximize the gains (distances shown the curves are scaled).

From figure 7 it can be concluded that for a fixed value of r_2 if the sum of the distances r_1 and r_3 increases G_p decreases however at the particular value of r_3 it becomes almost fixed. In figure 8 it is clear that for a fixed value of r_2 if

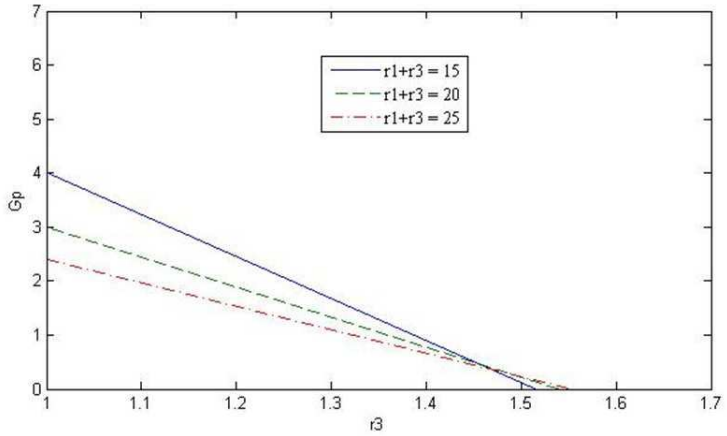

Fig. 7: *G_p vs r_3 curve*

the sum of the distances r_1 and r_3 increases G_{th} also increases however at the particular value of r_3 it becomes almost fixed. Considering these two graphs a trade-off between the gains and distance can be made.

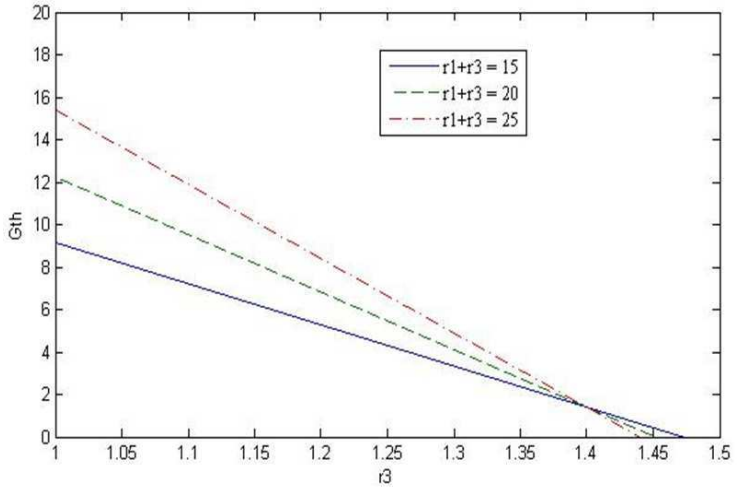

Fig. 8: *G_{th} vs r_3 curve*

Further work on this topic includes a more complex model having multiple transmitter and receiver and effect of different modulation technique and cross layer approach for further modification of the cooperative system.

References

[1] I. Cerutti, A. Fumagalli, and P. Gupta. Delay Models of Single-Source Single-Relay Cooperative ARQ Protocols in Slotted Radio Networks With Poisson Frame Arrivals. *IEEE/ACM TRANSACTIONS ON NETWORKING*, 16(2), April 2008.

[2] T. M. Cover and A. A. El Gamal. Capacity theorems for the relay channel. *IEEE Trans. Inf. Theory*, 25(5), 1979.

[3] A. Goldsmith. WIRELESS COMMUNICATIONS. Cambridge University Press, 2005.

[4] J. N. Laneman, G. W. Wornell, and D. N. C. Tse. An efficient protocol for realizing cooperative diversity in wireless networks. In *Proc. IEEE ISIT*, 2001.

[5] J. Morillo-Pozo, D. Fusté-Vilella, and J. García-Vidal. COOPERATIVE WIRELESS COMMUNICATIONS. CRC Press, 2009.

[6] T. S. Rappaport. Wireless Communications. Principles and Practice, Englewood Cliffs, NJ: Prentice Hall, 1996.

[7] M. Richaria. Satellite Communications Systems: Design Principles. McGraw-Hill Telecommunications, 1998.

[8] N. Wisitpongphan et al. QoS Provisioning using BER-Based Routing in Ad Hoc Wireless Networks. IEEE, 2005.

[9] E. Zimmermann, P. Herhold, and G. Fettweis. The impact of cooperation on diversity-exploiting protocols. In *Proc. 59th IEEE Vehicular Technology Conf.(VTC Spring)*, 2004.

Applicability of Recurring Patterns in Interference for Route Optimization in Mesh Networks

Till Wollenberg, Thomas Mundt
University of Rostock, Germany
Department of Computer Science
till.wollenberg@uni-rostock.de, thm@informatik.uni-rostock.de

Abstract

The basic idea presented in this paper is to use interference aware routing with predicted interference. Noise and other values are measured over a long time and within a wide area in order to find recurring patterns. Routing parameters are then adjusted according to these patterns. The objective is to improve the general network performance without permanently transmitting status information. In contrast to this, a predefined schedule derived from predicted interference is deployed once and updated only from time to time, thus reducing the overhead for network control. In this paper we introduce the new idea in general and investigate pattern recognition within the noise values for its suitability.

Acknowledgement: Parts of this paper have been taken over from a joint publication [26].

1 Introduction

As radio networks undergo constant changes, ad-hoc networks require dynamic routing and consequently appropriate routing protocols. Dynamic routing induces a significant overhead. Typical approaches are reactive and pro-active routing schemes. Several routing algorithms with different cost factors have been developed. Cost factors can be path loss, hop count, geographic location, and interference.

Instead of exchanging routing information in a highly dynamic manner, we propose a new approach to optimize routing. The optimization is very “cheap”

to achieve in terms of network overhead. We do not propose a completely novel routing algorithm itself but propose to amend routing algorithms in order to become aware of predictable congestion. This can be realized by adding an interference dependent value to the cost functions of relevant routing algorithms. Open questions to be answered in this context are:

- Is interference a local phenomenon in an ad-hoc network? Otherwise, diversions around locally contaminated areas would not be useful.
- Are there recurring patterns usable to predict interference levels?
- Are the changes in interference time series strong enough to generate a significant effect on network QoS parameters (is there enough amplitude)?

We assume, that routing conditions within the network follow a recurring pattern, for instance fluctuations of interference levels during each day. We further assume that routing algorithms can be tuned by considering these recurring patterns. The verification of these assumptions is the objective of this paper. Collecting information about typical network conditions (also called "experience") allows routers to avoid congestion. This is very similar to street traffic, where experienced drivers know when it is best to avoid certain roads, for instance during rush hour. The actual routing algorithm can be manipulated according to current network conditions. We concentrate on interference in this paper since this is the main cause of bandwidth limitation in radio networks and mainly all other parameters can be derived from interference[27]. The following steps are performed for the proposed optimization:

- **Collection of data** - A trade-off between overhead for collecting data and the necessary frequency and amount of data to recognize patterns has to be found. In most cases high granular sampling - for instance every 5 minutes - is sufficient. Data could be delivered for central processing during times of low network utilization. This is a strong benefit against highly dynamic routing protocols with much higher and permanent overhead.
- **Processing of data, pattern recognition, and prediction of interference** - Recurring pattern in courses of interference will be used to forecast the course of interference at all nodes (in the entire area of the network).
- **Calculating a schedule** - Routing parameters of all nodes within the ad-hoc network have to be optimized based on predicted interference.
- **Delivery of schedules to nodes** - This will be executed during calm network periods in order to avoid unnecessary network traffic (overhead).

- **Adjusting routing parameters** - Routing parameters have to reflect interference according to the schedule. This step delivers feedback, which is intended to tune the routing algorithm.

We collected over 1.2 million measurement reports from 50 different nodes. Each report contains the current noise at this node. Values are delivered by the network interface card itself. All values are uncalibrated. The nodes are distributed within a productive ad-hoc[1] network with about 200 nodes. The network spreads an area of about 20×10km in a mid-size city (Rostock, Germany, 200,000 inhabitants). The ad-hoc network is actively supported by the authors of this paper. Participating nodes delivered a report every 5 minutes. Each report includes a noise value supplied by the driver of the radio network interface. These data have been evaluated for the three questions mentioned before. In the remainder of this paper, we present the state of the art in relevant topics in section 2, show our idea of interference aware route optimizations in section 3. In a first step towards implementation, we examine collected values describing the noise at different nodes in order to infer a schedule in section 4. Conclusion and outlook are given in the last section 5.

A proof of the entire concept will require more research - such as simulations and implementations - and is not part of this paper. Research goes on while publishing first results. The paper evaluates necessary preconditions for interference aware routing with predicted interference values.

2 Technological basis

2.1 Effects of interference and interference avoidance

Calculations about how different interference levels influence the available bandwidth of a radio link have been published in [8]. Interference effects on throughput are discussed in [27]. Interference relevant to the link layer is often expressed as signal-to-noise ratio (SNR). Also according to [19] there is a high correlation between SNR and link quality. Throughput measurements are presented in [24].

The concrete throughput depends on some other network parameters as well. For our target network [27] provides good hints that throughput nonlinearly increases from 0 to 5000kbps at an SNR between 10 and 20dB within an IEEE 802.11g WLAN. The highest gradient of bandwidth over SNR is about 1.6Mbps per dB. The relation between SNR, data rate, and Packet Error Rate is described

[1] The investigated network [1] is considered an ad-hoc network since nodes may join or leave at any time and there is no central management. Most nodes are using the 802.11 ad-hoc mode, too.

in [7]. For comparison, the SNR reported by the driver of the network interface card varies about 2dB at a typical node of the network under investigation in this paper. Notice, that all values are delivered by the network interface card itself, which is neither calibrated nor supposed to be accurate. Although individual SNR values alone do not describe the wireless channel quality adequately, prior research shown before leaves good chances for interference controlled diversions around contaminated areas to work.

2.2 Interference aware routing

Typical cost factors or metrics in mobile ad-hoc networks are *hop count* (such as in AODV [18] and the RFC variant of OLSR [5]), and *path loss* (such as in OLSR LQ EXT Extension [10]). Examples for external parameters to be adapted in routing algorithms are *WILLINGNESS* (OLSR) as well as *TTL_INCREMENT, TTL_START, and TTL_THRESHOLD* (AODV). Changing the transmission power in a radio network is also used for topology control [2]. Direct integration of interference as a weighted cost factor into a modified routing algorithm would be another alternative [28, 4].

We focus on finding long term patterns in interference. Interference can have many sources, some of them are natural, the majority is generated by human activities. Interference affects the performance of radio networks and limits the available bandwidth. Avoiding regions with high interference levels promises a benefit of performance for the network user.

Interference aware routing helps avoiding highly "contaminated" areas. A variety of improvements has been proposed during the last years [22, 21, 6, 12]. Available protocols and metrics are NAVC and DIAR [11]. An example, how interference awareness can be added to an existing routing protocol is described in [15] and [16]. Simulation results for OLSR are presented in [14].

A major problem of interference aware routing is that adjustments in the network require that messages are sent over the network itself. Hence, all routing approaches have to take this into account in order to avoid oscillating routes and repeating topology changes which require further messages.

2.3 Interference forecast

This paper investigates whether changes of interference are predictable. As mentioned before, interference levels have a significant impact on reachable network performance.

Forecasting phenomena works more sufficiently when the source is known. Electromagnetic interference is caused by unwanted electromagnetic radiation from an external source. Natural sources could be sun eruptions or the Northern Lights. Sources of electronic noise are thermal noise, flicker noise and generation-recombination noise [23]. The main input of interference in the scenario are other WLAN stations working in the same frequency band. In this case, both the 2.4 GHz and the 5 GHz ISM bands are used. Other external signal sources are microwaves, radar etc. [13, 17].

Human beings adhere to certain schedules during a day. As using a wireless network and other transmitters in the relevant bands is more common during certain times of the day, changes of interference levels are supposed to be predictable [9] [8]. Typical period lengths found in other publications [25] are one day, and one week. Own research in the remainder of this paper will show, whether periodic changes of interference are predictable.

3 Interference aware route optimization with predicted network conditions

Overview and background: Figure 1 shows a cut-out of a chart depicting a so-called roof top network with about 200 nodes in the area of Rostock, Germany [1]. Commercial hardware is used, mainly WLAN routers with 2.4GHz interfaces for the respective ISM-band. The three most common hardware types are Linksys WRT54 in several variants, Buffalo WHR-G54, and Asus WL-500. The network provides network access to about 130 users. Main usage is accessing the internet. All nodes in the 2.4GHz domain are working in ad-hoc mode and hence sharing a single channel. Within the network several gateways provide access to the internet. The network could be specified as a multihop ad-hoc access network [3]. Some users are living in suburbs and nearby villages where high-speed data links are not available otherwise. These remote spots are connected to the core network by several dedicated links in the 5GHz ISM band. Separated 5GHz links are also used in an overlay network structure. This significantly reduces the number of hops between users and internet gateways. 5GHz links are built by several hardware interfaces, such as Atheros 5313.

OLSR is used as routing protocol within the entire network on all links. Path loss is used as routing parameter. OLSR is standardized in [5], but a slightly different implementation is used [10]. Since the majority of nodes is stationary due to the specific nature of a roof top network (except some mobile nodes such as notebook computers) the parameters of OLSR are tuned accordingly. For instance, update frequency of topology change messages is reduced. Hence, the overhead imposed by route updates is limited. Finding optimal paths in

Fig. 1: *Cut-out showing a central region of the investigated ad-hoc network. (Source: Opennet, OpenStreetMap)*

an ad-hoc network is almost impossible due to changes of radio conditions. An elementary topology control [20] is implemented by reducing the transmit power of nodes in densely populated areas with a high link-to-node ratio. Since interference is the prime reason for limited bandwidth, reducing interference is inevitable to increase throughput. Every transmission in a single frequency ad-hoc network induces interference for all other nodes. The level of interference depends mainly on the distance between interfering transmitter and receiver. Considering path loss as the only routing parameter will lead to some routes directly through jammed areas, which will further increase the interference and with certain probability increase packet loss in these areas after the routing decision has been made. An adapted routing algorithm could avoid areas of high interference instead of depending on path loss alone.

We assume, that significant patterns which might be detectable in altering interference levels are usable for look ahead planning of broad area traffic diversion around the affected areas. In order to find reoccurring increases or decreases of interference levels a search for periods in interference has to be performed. Suitable are especially those alterations which are limited to certain areas of the network. An overall increase of interference does not allow regional diversions. This leads to the need of comparing the progression of interference at different locations within the network.

Interference prognoses: Routing algorithms taking care of interference as main routing parameter have already been developed as shown in section 2. Interference aware routing requires knowledge about interference to be transmitted over the network, which will increase interference. As also shown in section 2 interference can have multiple sources. Some of these sources are candidates to reoccur with usable period lengths. We consider those period lengths as usable which cause a reappearing within a time span where the remaining configuration of the networks such as node locations and links stays stable within reasonable ranges. This means that the position of most of the nodes and links between them remain stable. Good candidates for period lengths are one day or one week. Longer period lengths are harder to detect and might be heterodyned by mid term changes of the network usage or by changes in the environment.

In this paper, we focus on the possibility to detect patterns in measured interference. The development of methods to adapt the routing will be discussed in later publications.

Collection of data: In order to find reoccurring patterns within interference values in time and space those values have to be collected. When implementing a routing algorithm that relies on predicted interference values instead of frequent updates of measurements the collection and distribution of these values should not lead to a large overhead. The possibility to collect those data all day round and to distribute them during times of lower network utilization is one major benefit of the new proposed method.

Processing data and searching for periodic events: Future interference values have to be predicted. This requires searching for periods within interference values, which is usually realized by performing a Fourier analysis. Usable period lengths are in the range of hours and days. It is evaluated in this paper that interference is a local phenomenon which allows diversions around contaminated areas.

Calculating a schedule and distributing it to the nodes: When periodic events have been found during data analysis, a general schedule for the entire network has to be calculated. The schedule contains traffic diversion in form of adjustments for the respective routing algorithm. A typical approach is changing the link weights. This schedule has to be delivered to all nodes, preferably during low traffic times.

Adjusting routing parameters: Routing parameters have to reflect interference according to the schedule. A feedback mechanism will provide constant readjustments.

4 Data analysis

A software program has been deployed on 50 nodes taking part in a test run. The clients have been installed by volunteers on their own nodes (the network consists of nodes owned by members. Hence, the selection of nodes is relatively arbitrary. Nevertheless, distribution and density of measuring nodes are sufficient for testing. The client retrieves interference values from the network interface card. All measurements rely on values reported by conventional network interface cards. Special equipment for calibration has not been used. Antenna gain and attenuation of cables etc. have not been considered.

Measurements are performed every 5 minutes. The current version of the client program delivers the measurement report directly to a server via HTTP. Productive versions will be able to store data over a day and deliver it to a processor during calm network conditions. A randomized latency (jitter) is used to prevent the server from synchronization effects. Figure 3 shows the interference level in a small part of the ad-hoc network within a four week randomly chosen time span.

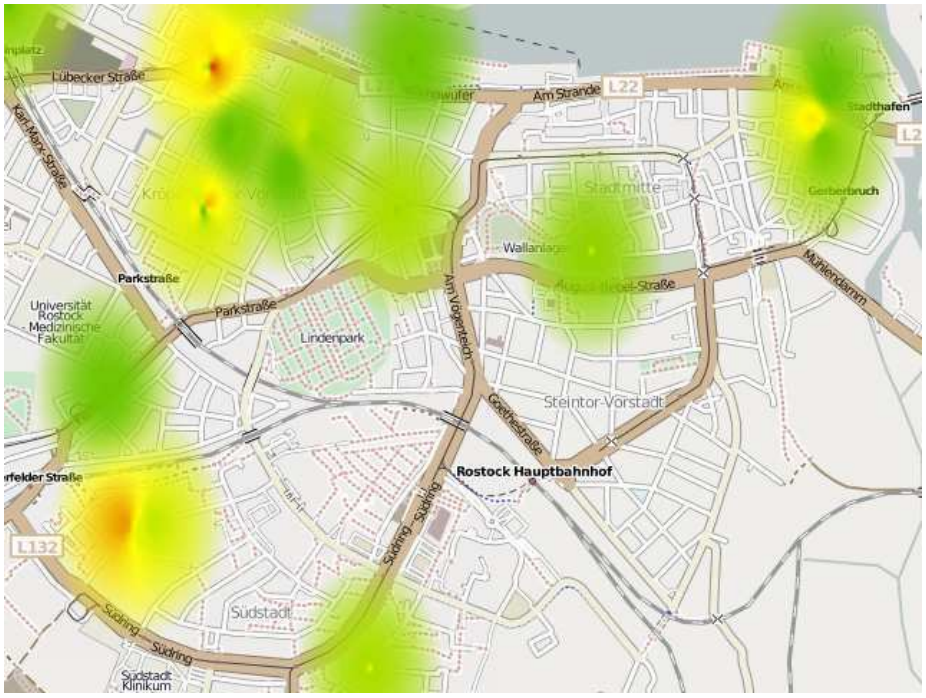

Fig. 2: *Geographical distribution of interference.*[2]

For this evaluation, a time span of 4 months between July and November 2008 has been considered. During this time more than 1.2 million measurement reports have been collected (note, that not all nodes delivered reports from the beginning and some of them were withdrawn). Most nodes delivered about 30,000 reports. Reports are stored in an RDBMS for convenient retrieval. [3] In order to find recurring patterns within the data some sample nodes have been chosen by calculating the variance within reported interference values. Figure 3 shows sample data for one node. For presentation purposes a low pass filter has been applied. At first sight, a daily course is visible, hence, a period length of one day is to be expected.

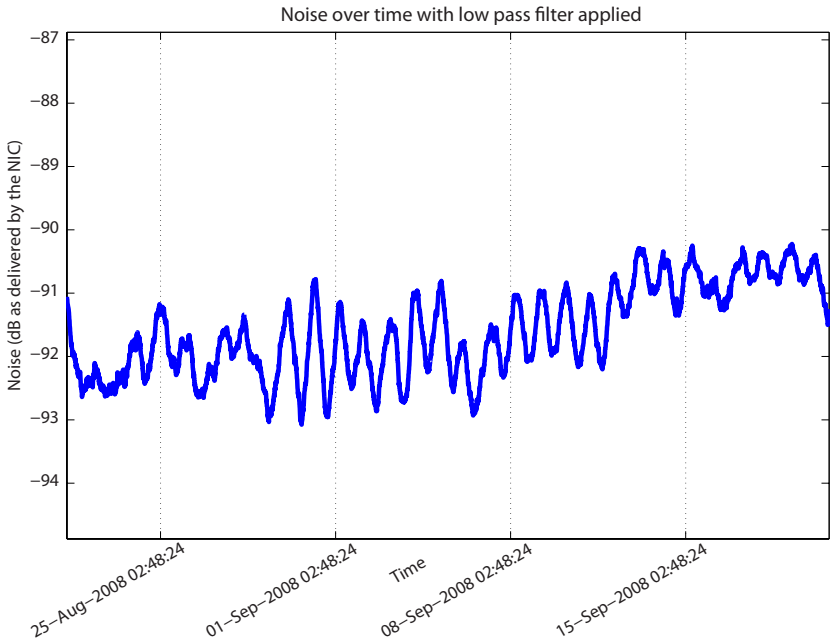

Fig. 3: *Measured noise over four weeks.*

A Fourier transformation delivers a significant peak at a period length of exactly one day. Figure 4 shows the period lengths found in fluctuating interference values measured at one node.

Two factors are important for our idea to work. Firstly, there are recurring patterns at one node. Secondly, those recurring courses are local phenomena. Otherwise, all nodes would suffer from the same increase of interference and deviations would become senseless.

[2]The figure depicts spatial interpolated noise values in dBm as reported by the network card's driver. This image and other images can be downloaded in full color and high resolution at `http://ox.informatik.uni-rostock.de/thm/olqm-figures/`

[3]All data are available for public download at `http://ox.informatik.uni-rostock.de/thm/olqm-data/` as time series in CSV format.

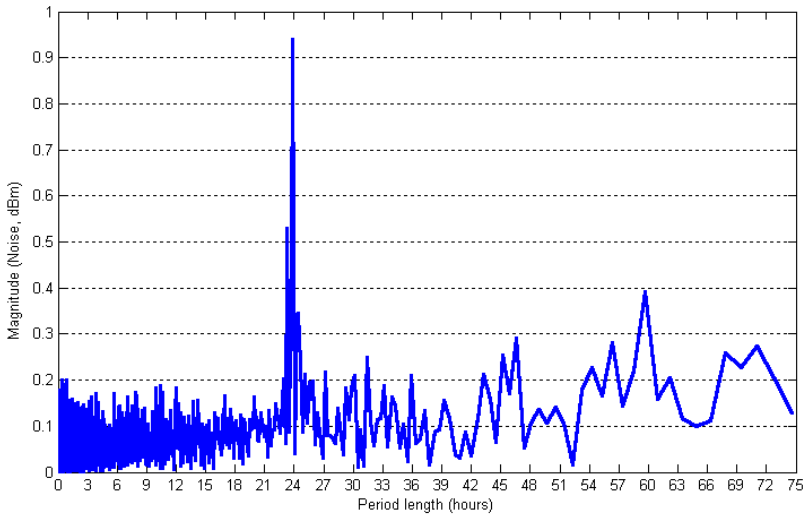

Fig. 4: *Period lengths found in the recorded data. (A 24h periodic signal is significant.)*

To test both conditions we have calculated the auto correlation of the noise values in the time domain and the cross correlation of noise values at different nodes at the same time. Figure 5 shows the course of interference values measured at two consecutive days at the same node.

A high correlation can be expected by looking at those mostly parallel courses. For more details, we have calculated all correlation coefficients for ten days in a row. These values are recorded in table 1.

To make correlation more visible, we have depicted those correlation coefficients in figure 6. In this example there is a strong correlation between most days, but for unknown reason Day 4 (Wednesday, 2008-July-09) has an untypical daily course of interference. There is no obvious reason for this to occur when looking at the day of week or the weather. This test has been successful in terms of finding recurring patterns usable for interference prediction. We collected measurement reports from about 50 nodes. We found that strong auto correlation between most days at almost every node. Results are representative for other nodes and reproducible for other times. Hence, interference prediction can be considered for long-term planning of traffic diversions around contaminated areas.

Most of the interference values at different nodes follow a daily pattern. For our purposes, those periodic events are usable when they occur at different times in different areas of the networks. Otherwise, the entire network would suffer

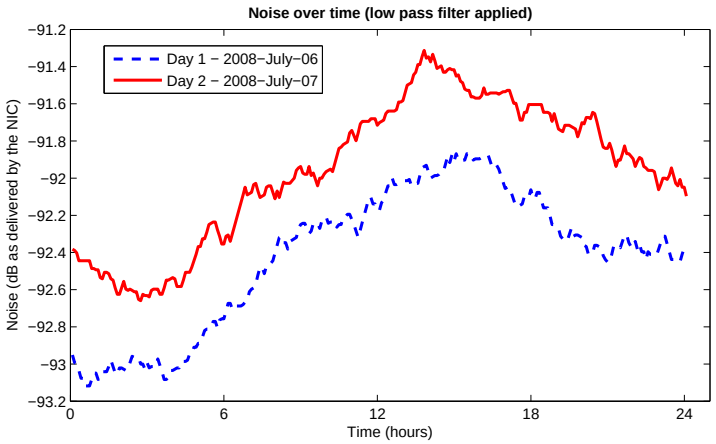

Fig. 5: *Course of interference at two consecutive days measured at one node.*

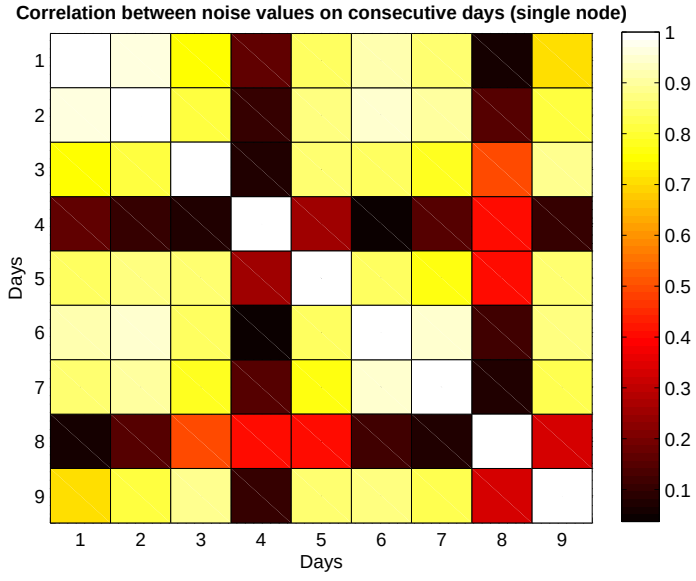

Fig. 6: *Correlation coefficients from table 1.*

Day	Day 1	2	3	4	5	6	7	8	9	10
1	1									
2	0.96	1								
3	0.76	0.81	1							
4	0.16	0.10	0.07	1						
5	0.84	0.88	0.86	0.26	1					
6	0.92	0.95	0.84	0.05	0.84	1				
7	0.86	0.90	0.78	0.16	0.76	0.95	1			
8	0.06	0.15	0.49	0.40	0.40	0.11	0.08	1		
9	0.71	0.81	0.88	0.11	0.85	0.87	0.83	0.33	1	
10	0.30	0.37	0.47	0.66	0.19	0.44	0.59	0.04	0.51	1

Tab. 1: *Correlation coefficients of daily courses of interference for ten consecutive days. (Example. Results are representative.)*

from increasing interference. Finding local phenomena offers a chance to divert traffic around contaminated areas. For this reason, we have conducted a cross-correlation analysis. Figure 7 shows about two weeks of interference values measured at two nodes within the network.

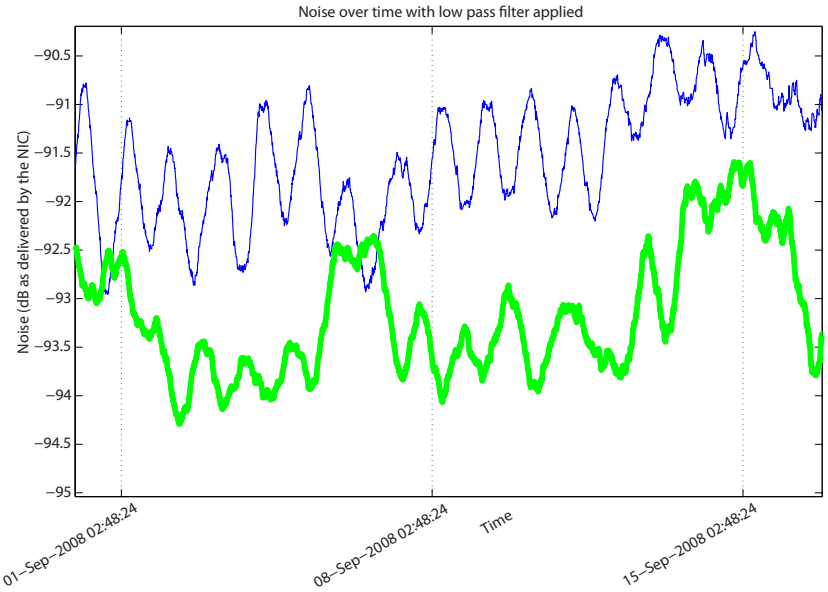

Fig. 7: *Courses of interference at two different nodes in the network. (Example.)*

	Day									
Day	1	2	3	4	5	6	7	8	9	10
1	0.51	0.77	0.19	0.05	0.56	0.76	0.19	0.27	0.54	0.36
2	0.50	0.81	0.27	0.08	0.52	0.77	0.34	0.25	0.60	0.43
3	0.57	0.78	0.60	0.45	0.27	0.62	0.63	0.01	0.56	0.60
4	0.72	0.33	0.34	0.51	0.38	0.02	0.45	0.62	0.48	0.24
5	0.71	0.63	0.33	0.22	0.56	0.59	0.30	0.33	0.40	0.65
6	0.44	0.86	0.38	0.18	0.41	0.81	0.46	0.14	0.67	0.44
7	0.28	0.91	0.41	0.24	0.27	0.84	0.52	0.04	0.78	0.28
8	0.63	0.02	0.30	0.33	0.08	0.01	0.40	0.12	0.07	0.46
9	0.40	0.81	0.58	0.53	0.25	0.63	0.65	0.01	0.66	0.56
10	0.40	0.81	0.61	0.66	0.33	0.46	0.77	0.71	0.87	0.15

Tab. 2: *Cross correlation of interference values in the time domain for two nodes. Daily courses are cross correlated.*

To gain more precise and comparable results we have determined cross-correlation coefficients for parallel time courses at different nodes. Example results are recorded in table 2. Results are representative for other pairs of nodes.

For better visibility, figure 8 depicts the values of table 2 graphically. In general, the cross correlation between different courses of interference in the time domain at two nodes is much weaker that auto correlation at one single node.

5 Conclusion

We presented the general idea of interference aware route optimization with predicted network conditions. We did not show that the idea itself will work. However, we did show that necessary preconditions are fulfilled. Finding a strong daily recurring pattern of interference values makes further research expedient.

The questions from section 1 can be answered as follows:

- Interference is a local phenomenon in an ad-hoc network. Cross-correlation between interference values of nodes in different areas is very low.
- There are recurring patterns usable to predict interference levels. A daily course (24h period length) had been substantiated by a spectrum analysis. Auto-correlation is very high.

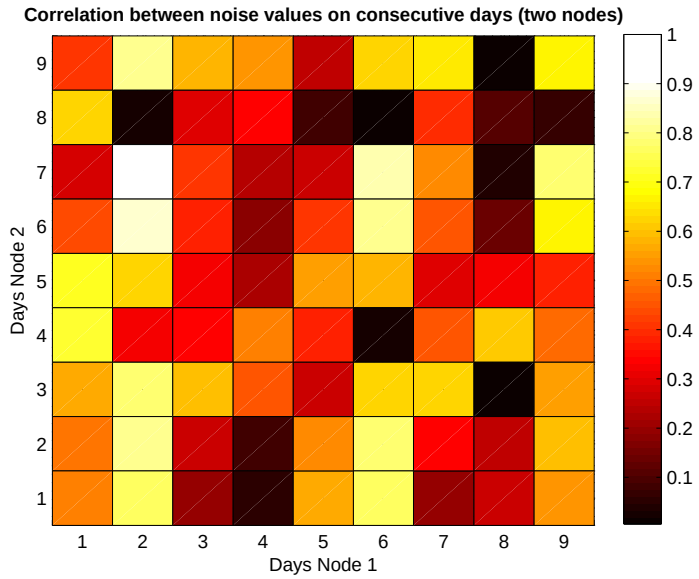

Fig. 8: *Cross correlation coefficients from table 2.*

- The difference between highest and lowest daily interference levels is usually at or above 2dB. This is high enough to have a significant impact on network QoS parameters.

By considering more than 1.2 million measurement reports from about 50 nodes we found a typical period length of 24 hours. The daily amplitude of interference values is relatively low. Prior research has shown that even with those small amplitudes interference aware routing increases throughput significantly and reduces packet loss. Further research is necessary for evaluating our idea.

References

[1] Opennet rooftop network. http://www.on-i.de/.

[2] D. Avidor, S. Mukherjee, and F.A. Onat. Transmit power distribution of wireless ad hoc networks with topology control. In *Proc. INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 46–52, 6–12 May 2007.

[3] J. Broch, D.A. Maltz, D.B. Johnson, Y.C. Hu, and J. Jetcheva. A performance comparison of multi-hop wireless ad hoc network routing protocols. In *Proceedings of the 4th annual ACM/IEEE international conference on*

Mobile computing and networking, pages 85–97. ACM Press New York, NY, USA, 1998.

[4] M. Canales, J.R. Gallego, A. Hernandez-Solana, and A. Valdovinos. Interference-aware routing with bandwidth requirements in mobile ad hoc networks. In *Proc. VTC-2005-Fall Vehicular Technology Conference 2005 IEEE 62nd*, volume 4, pages 2556–2560, 2005.

[5] T. Clausen and P. Jacquet. Optimized link state routing protocol (olsr). RFC3626, October 2003. http://www.ietf.org/rfc/rfc3626.txt.

[6] R. Gupta, Z. Jia, T. Tung, and J. Walrand. Interference-aware QoS Routing (IQRouting) for Ad-Hoc Networks. *Proceedings Globecom 2005*, 2005.

[7] M.J. Ho, J. Wang, K. Shelby, and H. Haisch. IEEE 802.11 g OFDM WLAN throughput performance. In *Vehicular Technology Conference, 2003. VTC 2003-Fall. 2003 IEEE 58th*, volume 4, 2003.

[8] K. Jain, J. Padhye, V.N. Padmanabhan, and L. Qiu. Impact of Interference on Multi-Hop Wireless Network Performance. *Wireless Networks*, 11(4):471–487, 2005.

[9] A. Kamerman and N. Erkocevic. Microwave oven interference on wireless LANs operating in the 2.4 GHz ISM band. In *Personal, Indoor and Mobile Radio Communications, 1997.'Waves of the Year 2000'. PIMRC'97., The 8th IEEE International Symposium on*, volume 3, 1997.

[10] Th. Lopatic. olsrd link quality extensions. http://www.olsr.org/docs/README-Link-Quality.html.

[11] L. Ma, Q. Zhang, F. An, and X. Cheng. DIAR: A Dynamic Interference Aware Routing Protocol for IEEE 802.11-Based Mobile Ad Hoc Networks. *LECTURE NOTES IN COMPUTER SCIENCE*, 3794:508, 2005.

[12] L. Ma, Q. Zhang, Y. Xiong, and W. Zhu. Interference aware metric for dense multi-hop wireless networks. In *IEEE International Conference on Communications (ICC 2005)*, 2005.

[13] S. Miyamoto, Y. Yamanaka, T. Shinozuka, and N. Morinaga. A Study of the Effect of Microwave Oven Interference on the Performance of Digital Radio Communications Systems.

[14] D.Q. Nguyen and P. Minet. Interference Effects on the OLSR Protocol: NS-2 Simulation Results. In *Third Annual Mediterranean Ad Hoc Networking Workshop, June 2004, Bodrum Turkey*. Med-Hoc-Net, 2004.

[15] D.Q. Nguyen and P. Minet. Interference-Aware QoS OLSR for Mobile Ad-Hoc Network Routing. *Proceeding of SNPD/SAWN*, 5:428–435, 2005.

[16] D.Q. Nguyen and P. Minet. Optimized Flooding and Interference-Aware QoS Routing in OLSR. In *Challenges in Ad Hoc Networking: Fourth Annual Mediterranean Ad Hoc Networking Workshop, June 21-24, 2005, Île de Porquerolles, France*. Springer, 2006.

[17] J. Padhye, S. Agarwal, V.N. Padmanabhan, L. Qiu, A. Rao, and B. Zill. Estimation of link interference in static multi-hop wireless networks. In *Proceedings of the Internet Measurement Conference 2005 on Internet Measurement Conference table of contents*, pages 28–28. USENIX Association Berkeley, CA, USA, 2005.

[18] C. Perkins and S. Das. Ad hoc on-demand distance vector (aodv) routing. RFC3561, July 2003. http://www.ietf.org/rfc/rfc3561.txt.

[19] D. Qiao and S. Choi. Goodput enhancement of IEEE 802.11 a wireless LAN via linkadaptation. In *Communications, 2001. ICC 2001. IEEE International Conference on*, volume 7, 2001.

[20] R. Ramanathan and R. Rosales-Hain. Topology control of multihop wireless networks using transmit poweradjustment. In *INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, volume 2, 2000.

[21] J. Tang, G. Xue, C. Chandler, and W. Zhang. Interference-Aware Routing in Multihop Wireless Networks using Directional Antennas. In *IEEE INFOCOM*, volume 1, page 751. INSTITUTE OF ELECTRICAL ENGINEERS INC (IEEE), 2005.

[22] J. Tang, G. Xue, and W. Zhang. Interference-aware topology control and QoS routing in multi-channel wireless mesh networks. In *Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, pages 68–77. ACM New York, NY, USA, 2005.

[23] Ralph E. Taylor. *Radio frequency interference handbook.* Washington Scientific and Technical Information Office, National Aeronautics and Space Administration, 1971.

[24] A.L. Wijesinha, Y. Song, M. Krishnan, V. Mathur, J. Ahn, and V. Shyamasundar. Throughput Measurement for UDP Traffic in an IEEE 802.11 g WLAN. In *Proc. of 6th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks (SNPD/SAWN'05), Towson, MD, USA*, pages 220–225, 2005.

[25] A. Willig, M. Kubisch, C. Hoene, and A. Wolisz. Measurements of a wireless link in an industrial environment using an IEEE 802.11-compliant physical layer. *Industrial Electronics, IEEE Transactions on*, 49(6):1265–1282, 2002.

[26] Till Wollenberg and Thomas Mundt. Interference aware route optimization with predicted network conditions - extended abstract. In *CNSR '09: Proceedings of the 2009 Seventh Annual Communication Networks and Services Research Conference*, pages 455–457, Washington, DC, USA, 2009. IEEE Computer Society.

[27] J. Zhang and I. Marsic. Link Quality and Signal-to-Noise Ratio in 802.11 WLAN with Fading: A Time-Series Analysis. In *Vehicular Technology Conference, 2006. VTC-2006 Fall. 2006 IEEE 64th*, pages 1–5, 2006.

[28] Xinming Zhang, Qiong Liu, Dong Shi, Yongzhen Liu, and Xiang Yu. An average link interference-aware routing protocol for mobile ad hoc networks. *Wireless and Mobile Communications, International Conference on*, 0:10, 2007.

A Comparison of Software Pseudorandom Number Generators

Dan Bogdanov, Riivo Talviste
University of Tartu, Estonia
Institute of Computer Science
db@ut.ee, riivo_t@ut.ee

Abstract

Random number generators are used in most cryptographic algorithms. The security of cryptographic primitives often directly depends on the unpredictability of the random number generator. The performance of the generator is also an important factor for creating efficient applications. This paper discusses several software-based pseudorandom number generators and analyses their security and generation speed. Based on the experimental results we choose two generators and use them in the SHAREMIND privacy-preserving virtual machine. We measure the effect the different generators have on the computation performance of SHAREMIND.

1 Introduction

Cryptography is used more and more in our everyday life. Many web connections are secured with the HTTPS protocol and people use them to log on to online banking systems and e-commerce sites. Several countries have rolled out electronic ID systems that allow citizens to identify themselves in e-government systems and give digital signatures on documents. In all these applications we rely on cryptography to provide us with a variety of security guarantees.

While a lot of effort goes into implementing secure encryption algorithms and cryptographic protocols, the security features of random number generators (RNGs) are similarly important. The majority of cryptographic algorithms and protocols require random nonces for operation. The security of the whole cryptographic primitive may depend on the infeasibility of guessing these random numbers. An adversary may find it easier to crack the underlying RNG than the

algorithm using it [11]. For that matter, *cryptographically secure random number generators* are distinguished to be sufficiently secure for use in cryptographic applications.

Furthermore, the performance of an RNG may also be an important factor in certain applications like secure multi-party computation. Also, encryption algorithms and cryptographic protocols are intensely used in server hardware and communication equipment. Hence, the generation of randomness should not be a bottleneck. There are specialized hardware components for performing hardware-accelerated encryption, that are used in servers. However, they does not solve the problem for personal computers and embedded systems. For this reason, software-based randomness generation is an important study area.

2 Contribution and outline

In this paper we select some freely available pseudorandom number generator (PRNG) techniques and analyse them considering security and performance. In Section 3 we give a brief overview of how random number generation works in general. In Section 4 we look at each PRNG separately and discuss its security. We also let each PRNG produce a certain amount of random data and compare their execution time.

In Section 5 we describe how the performance of a generator may affect actual applications. We show how changing the randomness generation method in the SHAREMIND privacy-preserving virtual machine [8] resulted in a significant performance improvement.

3 Random number generation

The best way to obtain unpredictable random numbers is to measure some kind of physical phenomena such as radioactive decay, thermal noise in semiconductors or radio waves from the space. Unfortunately, these kinds of measurements require specialized hardware and thus are not suitable for everyday use in servers and desktop computers. There are promising developments, like the AES-NI instruction set in the Westmere line of processors developed by Intel [1]. Hardware-accelerated AES will allow computers using these processors to run block cipher-based randomness generators considerably faster. Still, it will take time until the majority of machines have such capabilities.

There are some methods for acquiring entropy by sampling processes like the timing of hard disk drive operations or time intervals between keystrokes and mouse movements. However, these measurements expect the RNG to have a low-level access to device drivers [11, 10]. When using these methods one must also carefully assess, how much entropy can be extracted from these events, as seemingly random movements of the hand may in fact contain little randomness due to the way the human brain works.

Usually operating systems provide user applications with an interface to an RNG that generates cryptographically secure random numbers. This is possible because the operating system kernel has low-level access to device drivers and can collect entropy from various sources. This kind of RNGs can be either blocking or non-blocking. If a blocking RNG runs out of random data, then the applications using it have to wait until it can refill its entropy pool. Non-blocking RNGs use random values from blocking RNGs and specific algorithms to increase the amount of random data in their pool. Most common operating system provided RNGs are `/dev/random` (blocking) and `/dev/urandom` (non-blocking) in Linux systems and the CryptoAPI in Microsoft Windows systems.

Another way to produce random numbers is to use software applications. There are two kinds of software-based random number generators: Deterministic Random Bit Generators (DRBGs), also known as Pseudorandom Number Generators (PRNGs), and Non-deterministic Random Bit Generators (NRBGs), also known as "true" Random Number Generators. According to the Information Technology Laboratory of National Institute of Standards and Technology, there are currently several approved DRBGs and no approved NRBGs [7]. In this paper we concentrate on pseudorandom number generators.

A PRNG is a function in the form

$$f : \mathcal{S} \to \mathcal{R}$$

where $\mathcal{S}$ is the set of possible *seeds* and $\mathcal{R}$ is the set of random values. Since PRNGs are deterministic, their security relies on the seed value. The random number generator uses a seed as an initial value to produce all subsequent values. The PRNG itself is deterministic, so an initial seed determines the output of the generator. Thus, the seed has to be chosen carefully so that the generated random values would be cryptographically secure. There are many examples [10, 12] where a poorly chosen seed has made the generated random values predictable. Typically, PRNGs are seeded with entropy collected using methods described above.

4 A comparison of generators

4.1 The testing environment

We selected a number of PRNG implementations for testing. The implementations are either standalone or from well-known libraries such as Crypto++, OpenSSL and the C++ standard library. For each PRNG, we implemented a benchmarking application in C++.

Each application measures the time it takes a certain PRNG to generate 1 MB of pseudorandom data. Each test is run 100 times and an arithmetic average is calculated from all run times. The execution times are measured in microseconds (μs). However, in Table 1 they are converted into milliseconds (ms) for readability.

The computer used for testing is a personal computer with an Intel Core 2 Duo CPU, running at 3.0 GHz and with 2.0 GB of RAM. The operating system used is 32-bit Microsoft Windows Vista. All tests are executed in the Cygwin environment version 1.7 and compiled with GCC version 4.3.2.

We will now describe the PRNG candidates in some detail.

4.2 C++ built-in random

The C++ programming language has a built-in PRNG function `rand()` declared in `stdlib.h`. It returns a pseudorandom integral number in the range 0 to `RAND_MAX` ≥ 32767. The constant `RAND_MAX` is also defined in `stdlib.h` [6].

The `rand()` function's algorithm uses a seed to generate a series of random numbers. The seed should be initialized with `srand()` function, which takes a constant value as an argument. The system time in milliseconds is most commonly used as an initial seed. It should be noted, that the C++ standard does not specify the algorithm to use to implement the method. Hence, random numbers generated by `rand()` are not considered cryptographically secure.

As seen from Table 1, C++ `rand()` function is fairly fast. The average time to generate 1 MB of random data is 1080 μm.

4.3 The Crypto++ library

The Crypto++ library [3] is a free open source C++ class library of cryptographic schemes. Among other algorithms, the Crypto+ library includes several pseudorandom number generators with different security levels. In this section we describe most of the provided generators. In our tests we used version 5.6.0 of the library, which we compiled under the aforementioned Cygwin environment.

4.3.1 LC_RNG

LC_RNG is an implementation of a linear congruential generator, which is not meant for use cryptographic applications [2]. The LC_RNG generator uses a fast algorithm and generates 1 MB of random data in 13800 μs (see Table 1).

4.3.2 RandomPool

The RandomPool is a PRNG that does not generate cryptographically secure random data by default. However, it can be used to generate cryptographically secure random data after seeding the pool with enough entropy by using the `IncorporateEntropy()` method. One can use `CanIncorporateEntropy()` to check if `IncorporateEntropy()` is implemented in the current environment [2]. The RandomPool is slower than the previous techniques.

4.3.3 AutoSeededRandomPool

The AutoSeededRandomPool generates cryptographically secure random data, as it seeds itself with an operating system provided RNG on startup. It can be seeded with both blocking and non-blocking RNGs [2]. In our test, we seed it with a non-blocking RNG, which is its default behaviour. Its performance is similar to the one of RandomPool.

4.3.4 AutoSeededX917RNG

AutoSeededX917RNG is a PRNG from ANSI X9.17 Appendix C. Like AutoSeededRandomPool, it is seeded using an operating system provided RNG, which makes it suitable for cryptographic use [2]. The generation itself is based on using a block cipher such as DES or AES in counter mode. Since block

ciphers are relatively slow when compared to linear congruential generators and stream ciphers, this generator has a lower performance.

4.4 The OpenSSL library

The OpenSSL library [5] is a free open source toolkit to implement the Secure Socket Layer (SSL v2/v3) and Transport Layer Security (TLS v1) protocols. It is also designed to be a general purpose cryptography library. It is widely usen in many applications. In our test we use OpenSSL library version 0.9.8k, precompiled for the Cygwin environment.

OpenSSL library provides PRNGs that are also used by other functions of the library. `RAND_pseudorandom_bytes()` generates pseudorandom bytes that should not be used for cryptographic key generation. `RAND_bytes()`, that we also use in our test, produces cryptographically secure random data when seeded with enough entropy. The entropy level of the PRNG can be increased by using functions in the OpenSSL library. For example, we could either mix some amount of memory into the entropy pool or collect entropy from Windows events or screen contents [4].

The generation algorithm of OpenSSL is more complex than in previous methods, so the performance is the slowest in our comparison.

4.5 The SNOW2 stream cipher

The SNOW 2 cipher [9] is a well-known stream cipher. A stream cipher works as follows. The cipher is given an initial vector and after that it starts outputting a stream of random bits that are combined with the input plaintext using the XOR operation. In that sense the stream cipher acts exactly the same way as a pseudorandom generator. In our experiment we consider the initial vector as the seed and use the output of the stream cipher to construct 32-bit random values.

Stream ciphers are used in mobile phones and protocol where high performance is important. It follows, that SNOW 2 is considerably faster than constructions based on a block cipher. Given that stream ciphers are used in demanding situations and no known good attacks are known at the time of writing of this paper, we consider SNOW 2 sufficient for use in applications like secure multiparty computation.

The SNOW 2 implementation is well-optimized and performs better than almost all the other generators. It is negligibly slower than the built-in generator of C++, but its security is significantly better.

4.6 Experimental results

The following table contains the performance results measured during the experiments.

PRNG name	Avg. time (ms)
C++ `rand()`	1.08
Crypto++ LC_RNG	13.80
Crypto++ RandomPool	1 124.80
Crypto++ AutoSeededRandomPool	1 117.73
Crypto++ AutoSeededX917RNG	1 224.82
OpenSSL `RAND_bytes()`	1 531.61
SNOW 2	1.48

Tab. 1: *The average time taken to generate 1 MB of randomness.*

5 Random number generators and secure multi-party computation

5.1 Principles of share computing

Secure multi-party computation is a cryptographic technique for performing secure function evaluation. In practice, this technique allows us to perform privacy-preserving data processing with very good security guarantees. However, this technique may require large quantities of randomness to provide privacy for the data. We will now describe how this works using the SHAREMIND system [8] as an example.

SHAREMIND is a *share computing* system. That is, it is based on the *additive secret sharing scheme*. If we want to process an input value s, we have

to distribute it into *shares*. Given a random generator $\mathcal{RNG}$ we perform the following steps:

$$s_1 \leftarrow \mathcal{RNG}$$
$$s_2 \leftarrow \mathcal{RNG}$$
$$s_3 = s - s_1 - s_2 \bmod 2^{32}$$

We now have shares s_1, s_2 and s_3 that represent the initial value s. If we distribute these to three separate parties, not one of them will know anything about s. In fact, it will be impossible to reconstruct s without access to all the shares. If we now share many values like this, we have created a private database. It is easy to see, that for each value shared, we need two random values. Since SHAREMIND operates with 32-bit integers, two 32-bit random values are required to securely store each value.

After we have securely stored the whole database we need to process the shared data. The parties holding the shares will exchange messages according to specific protocols. As a result, the parties will hold new shares that represent something computed from the inputs. These new shares can be used in further computations. Figure 1 illustrates this concept.

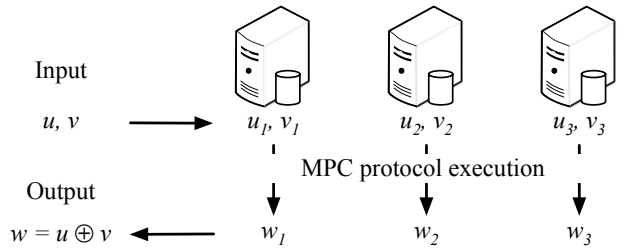

Fig. 1: *An example of a multi-party computation procedure.*

Such protocols require a way to hide the shares, as simply sending them to each other would compromise privacy. At this point SHAREMIND uses additional randomness to "hide" the shares. This randomness will be cancelled out during equations so that the protocol provides a correct result. The multiplication protocol in the current experimental version of SHAREMIND requires three additional random values for each operation. It follows that SHAREMIND requires new randomness continuously. Since SHAREMIND is designed to run data mining algorithms on large datasets, the number of operations and the required amount of random values will grow significantly.

5.2 Performance comparison

Before we started this work SHAREMIND used the AutoSeededX917RNG generator from the Crypto++ library. We performed benchmarks for two operations - multiplication and bitwise addition. While multiplication is one of the simplest share computing protocols implemented in the framework, bitwise addition is a more complex protocol that is a critical for performing comparisons. Both operations were benchmarked in their vectorized form, for SHAREMIND is designed to support single-instruction-multiple-data (SIMD) operations.

The results of the test are shown on Figure 2. The figure represents the time taken in specific protocol steps. The four protocol components that take significant time are randomness generation, waiting for messages, processing the queue of incoming messages and processing the queue of outgoing messages. The durations of the rest of the actions were insignificant. We see, that randomness generation takes up more than two thirds of the protocol execution time.

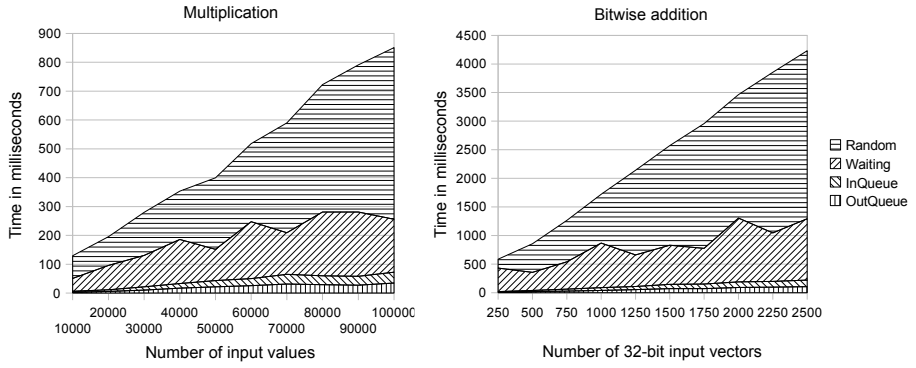

Fig. 2: SHAREMIND *performance using the AutoSeededX917RNG.*

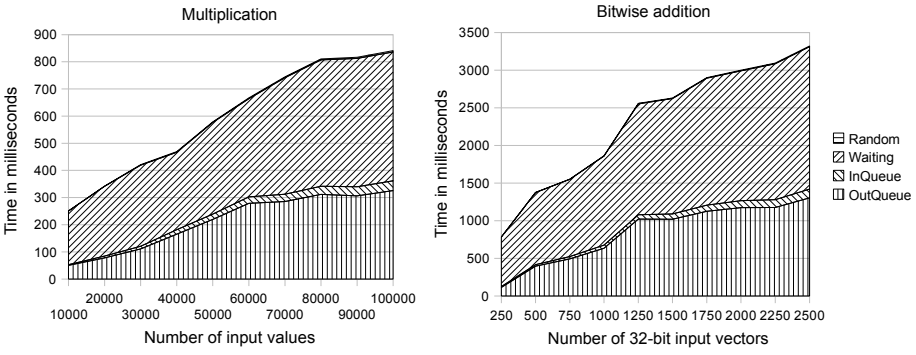

Fig. 3: SHAREMIND *performance using the SNOW 2 generator.*

Based on the performance results from this paper we implemented the SNOW 2 stream cipher as the randomness generator in SHAREMIND and ran the benchmarks again. The results can be seen on Figure 3. The time used generate randomness has decreased sharply, becoming insignificant when compared to the network wait time. However, the general operation performance has increased only slightly. This is caused by the fact that network traffic that was running in background with the previous generator still takes roughly the same time. Still—the bitwise addition protocol is slightly faster. Most importantly, we have removed a major bottleneck and found the next one. The next logical step is to see whether the network layer of SHAREMIND could be optimized to decrease the waiting times.

6 Conclusion

Cryptographic protocols have become an essential part of our everyday computer use. However, not all pseudorandom number generators produce unpredictable values that can be used in these protocols. In this paper we analyse some of the free open source PRNG libraries from the point of security and performance.

We found that while simple PRNG's work fairly fast, more secure generators take up to 1500 times more time to produce the same amount of random data. It is an important fact to take into account when building applications that make intensive use of software random number generators. If an application needs secure random values in huge quantities and faster than a software RNG can provide, then hardware security modules should be used.

We applied our findings on the randomness generators on the SHAREMIND virtual machine by replacing the AutoSeededX917RNG with the SNOW 2 stream cipher. While the overall performance did not change much, we did achieve noticeable changes in the protocol timings. The randomness generation is no longer a bottleneck in SHAREMIND and further optimizations in the networking layer may bring considerable improvements to the performance of the virtual machine.

References

[1] Advanced Encryption Standard (AES) Instructions Set Rev 2. Published online at `http://software.intel.com/en-us/articles/advanced-encryption-standard-aes-instructions-set/`. Last visited on Aug 3, 2009, 2009.

[2] Crypto++: Crypto++ Library 5.6.0 API Reference. Published online at `http://www.cryptopp.com/docs/ref/`. Last visited on July 31, 2009, 2009.

[3] Crypto++ Library 5.6.0 - a Free C++ Class Library of Cryptographic Schemes. Published online at `http://www.cryptopp.com/`. Last visited on July 31, 2009, 2009.

[4] OpenSSL: Documents, RAND_add(3). Published online at `http://www.openssl.org/docs/crypto/RAND_add.html`. Last visited on July 31, 2009, 2009.

[5] OpenSSL: The Open Source toolkit for SSL/TLS. Published online at `http://www.openssl.org/`. Last visited on July 31, 2009, 2009.

[6] rand - C++ Reference. Published online at `http://www.cplusplus.com/reference/clibrary/cstdlib/rand/`. Last visited on July 31, 2009, 2009.

[7] Random number generation. Published online at `http://csrc.nist.gov/groups/ST/toolkit/random_number.html`. Last visited on July 31, 2009, 2009.

[8] Dan Bogdanov, Sven Laur, and Jan Willemson. Sharemind: A framework for fast privacy-preserving computations. In Sushil Jajodia and Javier López, editors, *ESORICS*, volume 5283 of *Lecture Notes in Computer Science*, pages 192–206. Springer, 2008.

[9] Patrik Ekdahl and Thomas Johansson. A new version of the stream cipher snow. In *Proc. SAC 2002, volume 2595 of LNCS*, pages 47–61. Springer, 2002.

[10] Simson Garfinkel and Gene Spafford. *Practical Unix and Internet security (2nd ed.)*. O'Reilly & Associates, Inc., Sebastopol, CA, USA, 1996.

[11] Peter Gutmann. Software Generation of Practically Strong Random Numbers. In *In Proceedings of the 8th USENIX Security Symposium*, pages 243–257, 1998.

[12] J. Markoff. Security flaw is discovered in software used in shopping. *The New York Times*, 19, 1995.

Estimation of Doppler Shift for IEEE 802.11g Standard

Janis Jansons, Aleksandrs Ipatovs, Ernests Petersons
Riga Technical University, Latvia
Faculty of Electronics and Telecommunications
janis.jansons@rtu.lv, aleksandrs.ipatovs@riga.lv,
ernests.petersons@rtu.lv

Abstract

The common problem of the OFDM systems is the high sensitivity to frequency offset caused by tuning oscillator instabilities and Doppler shifts induced by the channel. Time variances of the channel during one OFDM symbol interval destroy the orthogonality of different subcarriers and generate power leakage among subcarriers, known as Inter-Carrier Interference (ICI). ICI in OFDM systems degrades the performance of both symbol detection and channel estimation. ICI produce phase noises which increase error vector magnitude (EVM) for conventional digital modulation methods such as phase-shift keying (PSK) and quadrature-amplitude modulation (QAM). The main focuses of this research are theoretically and practically evaluate the wireless local area network (WLAN) with Institute of Electrical and Electronics Engineers (IEEE) 802.11g standard in mobile environment such as vehicular to infrastructure (V2I) from Doppler Effect aspect.

1 Introduction

Short-range vehicle-roadside or V2I communication is expected to be a part of the future intelligent transportation system (ITS) in order to increase the safety of the roads and efficiency of the traffic. Therefore, investigation on proper communication for ITS is increasing. Today, the IEEE 802.11g standard for high data rate wireless networks is widespread and costs effective. Extension of this standard could be a part of V2I communication technology. The IEEE 802.11g is Orthogonal Frequency Division Multiplexing (OFDM) based standard. In OFDM, multiple frequency channels, known as sub-carriers, are orthogonal to

each other. Well known problem of OFDM is sensitivity to frequency offset between the transmitted and received signals, which may be caused by Doppler shift in the channel, or by the difference between the transmitter and receiver local oscillator frequencies. Carrier frequency offset causes loss of orthogonality between sub-carriers. Signals which are transmitted on each carrier are not depended from each other. That leads to inter-carrier interference (ICI). Some problems such as throughput, coverage range, Doppler shift, response times have to be solved before wireless vehicle-roadside infrastructure can be used on roads. In this paper an analysis of frequency offset caused by Doppler shift over experimental IEEE 802.11g wireless network is proposed.

2 802.11g-based Wireless LAN

Wireless Local Area Networks with IEEE 802.11g standard are most widespread today. 802.11g standard uses OFDM and Complementary Code Keying (CCK) to support higher raw data rate "over the air" (up to 54 Mbps) and rate in MAC Layer (up to 25 Mbps). OFDM is multi-carrier modulation which converts single high-rate bit stream to low-rate 64 parallel bit stream. Each sub-carrier can be modulated by binary phase-shift keying (BPSK), quadrature phase-shift keying (QPSK), 16-symbol quadrature amplitude modulation (16QAM), 64-symbol quadrature amplitude modulation (64QAM). To achieve high bandwidth efficiency, the spectrum of the sub-carriers with frequency spacing has to be closely spaced and overlapped. The OFDM symbols are generated using IFFT. Practically, OFDM symbol is sensitive to frequency offset [4]. On the receive side, a frequency offset correction scheme has to be used in addition. For 802.11g standard a receiver frequency tolerance which is equal with ± 60300 Hz is defined.

3 Doppler Shift

Doppler shift can cause significant problems if the transmission technique is sensitive to carrier frequency offsets or if the relative speed is too high. When an electromagnetic wave source and the receiver are moving relatively one to another, the received signal frequency will not be the same as the source signal frequency. When they are moving toward each other the frequency of the received signal is higher than the source frequency, but when they are moving from each other the frequency of the received signal is lower than the source frequency. This occurrence is called the Doppler shift. The amount of the Doppler shift depends on relative motion between source and receiver and on the speed of wave propagation. Maximal Doppler shift for frequency is calculated according to the formula:

$$f_d = \frac{v_r \cdot f_c}{c} \cos \alpha \tag{1}$$

where f_c is source frequency, v_r is the speed difference between objects, c is the speed of light ($3 \cdot 10^8$ m/s), and $\alpha \in [0, \pi]$ is the angle of the velocity vector. Our aim is to get maximal f_d which happens when $\alpha \to 0$. (1) can be changed to

$$f_d = \frac{v_r \cdot f_c}{3.6 \cdot 3 \cdot 10^8} \tag{2}$$

Values of f_d for 2.4 GHz carrier and various speeds are listed in Table 1. On the speed range from 10 km/h to 120 km/h the Doppler shift is from 20 Hz to 300 Hz.

V(km/h)	10	20	30	40	50	60	70	80	90	100	110	120
f_d(Hz)	22	44	66.7	88.9	111	133	155.6	177.8	200	222	244	266.7

Tab. 1: *Doppler shift for various speeds*

$$\mu = \frac{f_d}{f_c} \tag{3}$$

The relative Doppler shift (μ) is about 10^{-8} to 10^{-7}, which is very small. The fact that all subcarrier frequencies changes identically destroys the orthogonality between subcarriers [5] and generate power leakage among the subcarriers, known as ICI. Theoretical influence of maximal Doppler shift on 802.11g standard on the speed of vehicle from 10 till 120 km/h is very low. In this case it is possible analytically to determine the speed (v_r) of the vehicle when the affect of Doppler shift can influence on the signal:

$$v_r = \frac{f_d \cdot 3.6 \cdot 3 \cdot 10^8}{f_c} \tag{4}$$

4 Testing Environment and results

The goal of practical test was to investigate the possibility of 802.11g standard use in V2I practical environment from Doppler shift aspect. For assessing the quality of the OFDM signals we have measured error vector magnitude (EVM).

This measurement gives an overall view of quality of the modulated signal, which in turn gives a sense of how well the receiver would be able to receive and interpret the signal. This information is closely related to the physics layer of the system and gives a complete picture of the channel distortion. EVM can be more useful to the microwave engineer because it contains information about both amplitude and phase errors of the signal [2]. EVM is a measure for the difference between the theoretical wave and modified version of the measured waveform. The measured waveform is modified by first passing it through a specified receiver measuring filter. The EVM result is defined as the square root of the ratio of the mean error vector power to the mean reference signal power expressed as a percentage or dB. Mathematically, the error vector e can be written as

$$\underline{e} = \underline{w} - \underline{v} \tag{5}$$

Where $\underline{w}$ is the modified measured signal and $\underline{v}$ the ideal transmitted signal. The error vector $\underline{e}$ for a received symbol is graphically represented in figure 1.

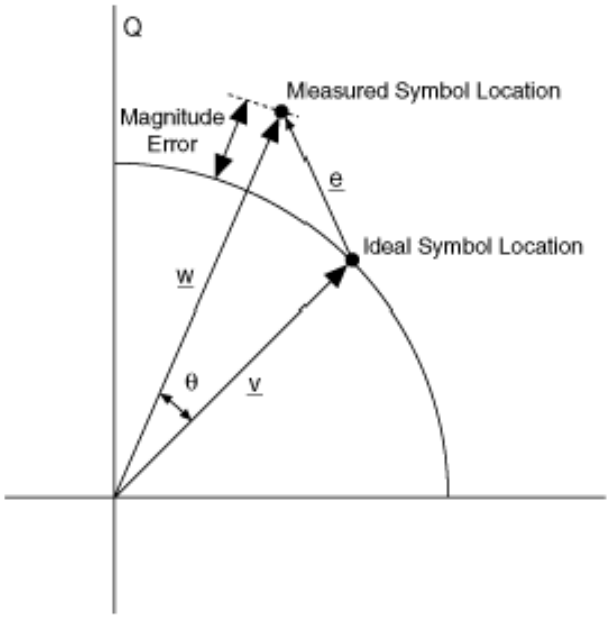

Fig. 1: *Representation of Error Vector*

EVM can be defined as

$$\sqrt{\frac{E[|\underline{e}|^2]}{E[|\underline{v}|^2]}} \tag{6}$$

The wireless link is highly influenced by their surrounding environment. Therefore the test bed was chosen carefully with no obstacle in the line of sight and no interfering wireless network in the neighborhood. For the experiments the airfield "Rumbula" in Riga city, Latvia (Fig. 2) was chosen.

Fig. 2: *Testing Location at the Airfield of Rumbula*

The nearest obstacle was 300-400 m away from the airfield surface and no other wireless networks could be detected. Additionally this place was chosen for vehicle safety reasons, because during the experiments the vehicle had to reach the speed of 120 km/h.

Fig. 3: *Signal transmitting side*

For the experimental signal generation in the test bed the vector signal generator R&S®SMBV100A was used. It was set on a moving vehicle (Fig. 3). Signal analyzer R&S FSV-K91n was used for wireless signal estimation (Fig. 4).

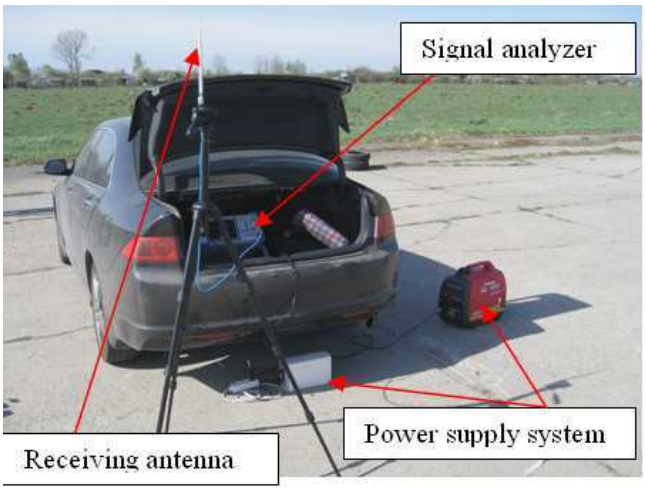

Fig. 4: *Signal receiving side*

Signal generator power supply was established by UPS APC 1000VA, but signal analyzer power supply was established by 2kW power generator with APC UPS (Fig. 4).

The focus was to set the best link with the highest signal transfer speed for OFDM 16-QAM (24Mbps) and for OFDM 64-QAM (54Mps) and optimal line of sight distance between receiving and transmitting sides (about 200 meters). For the experiment first channel (2.412 GHz) with signal output level +15 dBm was used. For the wireless measurements the sequence at fixed link-layer data rate 24 Mbps and 54 Mbps in 802.11g-only mode and with no automatic data rate adaptation was performed. In order to get right movement speed shown in table 1 for each measurement the moving vehicle with the signal generator was equipped with automatically controllable speed limiter.

Figures 5 and 6 shows data that was received on the Rohde&Schwarz FSV-K91n signal analyzer when vehicle speed was 20 km/h.

The Figure 5 or result summary list presents the overall measurement results and provides limit checking for result values in accordance with the 802.11g standard [1]. Result values which are within the limit as specified by the standard are displayed in green. Result values which are outside of the limits specified by the standard are displayed in red (not present in figure). Results which have no limits specified by the standard are displayed in white (bold). Limit values which are displayed in white (not bold) can be modified. The results displayed in this list are for the entire measurement. If a specific number of bursts have been requested which requires more than one sweep, the result summary list is updated at the end of each sweep. The number of bursts measured and

Fig. 5: *EVM estimation example on the Rohde&Schwarz FSV-K91n signal analyzer*

the number of bursts requested are displayed to show the progress through the measurement. The Min / Mean / Max columns show the minimum, mean or maximum values of the burst results.

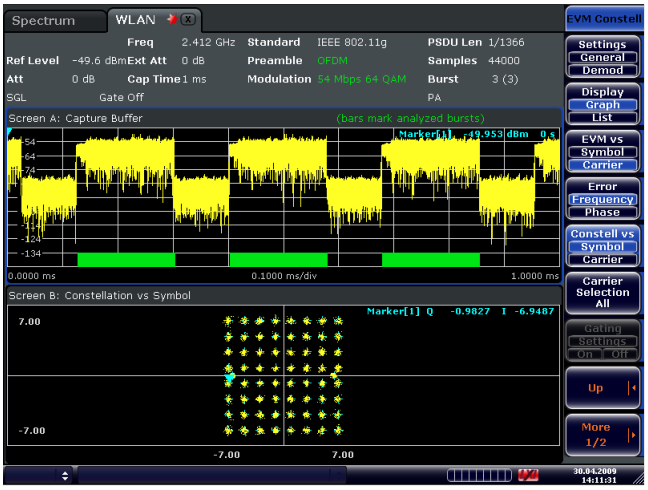

Fig. 6: *Signal constellation example on the R&S FSV-K91n signal analyzer*

Figure 6 is divided in two screens - the Magnitude Capture Buffer for all IQ measurements and the Constellation versus Symbol. The Magnitude Capture Buffer display shows the complete range of captured data for the last sweep. All analyzed bursts are identified with a green bar at the bottom of the Magnitude Capture Buffer display. The Constellation versus Symbol result screen shows

the in-phase and quadrature phase results over the full range of the measured input data.

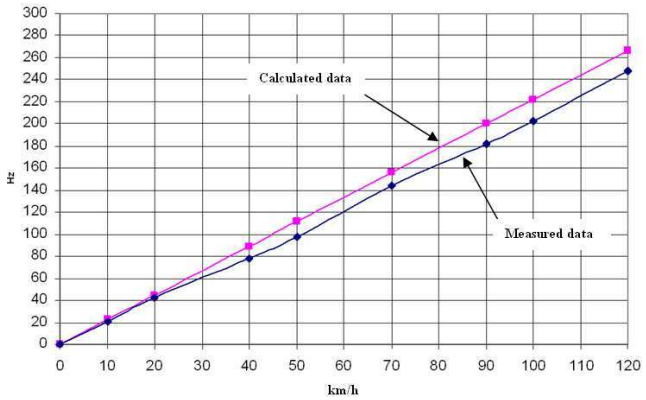

Fig. 7: *Doppler shift diagrams*

When all necessary measurements were made it is possible to analyze experimental data. Theoretical (red line) and practical (blue line) of Doppler shift are shown in Fig. 7. The difference between theoretical and practical data is small.

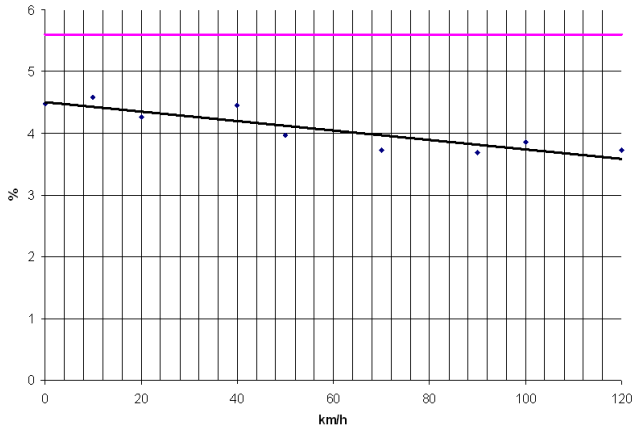

Fig. 8: *EVM (%) dependence from the vehicle speed and linear trend line*

In OFDM link sub-carriers are perfectly orthogonal only if transmitter and receiver use exactly the same frequencies. Any frequency offsets in Inter-Carrier Interference (ICI) [5] could increase EVM. The 802.11g standard have define EVM limits for each data rate (e.g. 54 Mbps EVM $<$ 5.6%, 24Mbps EVM $<$ 15.85%). Under the red line on figures 8 and 9 a field is shown that can satisfy the necessary link establishment to transfer correct data in wireless network. Figure 8 shows dependence of EVM from the vehicle speed on 54Mbps data

speed with 64-QAM. Average EVM on 10 km/h was 4.48% and on 120 km/h was 3.73%. The linear trend in figure 7 shows small EVM improvement on higher vehicle speed.

Figure 9 shows dependence of EVM from the vehicle speed on 24 Mbps 16-QAM. In this case EVM limit according to standard was three times greater than experimental EVM. Average EVM on 10 km/h was 4.57% and on 120 km/h was 4.03%.

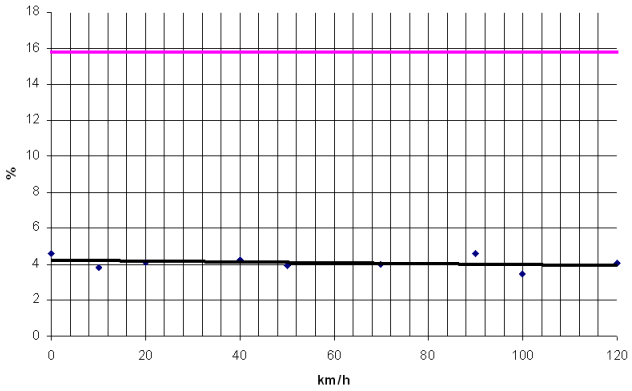

Fig. 9: *EVM (%) dependence from vehicle speed and linear trend line*

5 Conclusion

The main task of this research was to evaluate the Doppler shift impact on the 802.11 g V2I wireless mobile network. The main task was to prove that IEEE 802.11 g equipment with OFDM technology is sensitive against frequency offset [3] that caused power leakage between OFDM subcarriers on different vehicle speeds. This task was fulfilled completely.

After the summarizing of the theoretical and practical results fallowing conclusions came by: Doppler Effect influence on wireless network based on WLAN OFDM with IEEE 802.11 g standard technology were observed; Gained theoretical and practical results show that WLAN OFDM with IEEE 802.11g technology is consistent against channel time dispersion which can appear while vehicle is moving.

References

[1] IEEE Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher-Speed Physical Layer Extension in the 2.4 Ghz Band, IEEE Standard 802.11g-2003.

[2] M. D. McKinley, K.A. Remley, M. Myslinski, J.S. Kenney, D. Schreurs, and B. Nauwelaers. EVM calculation for broadband modulated signals. *64th ARFTG Conf. Dig.*, pages 45–52, Orlando, FL, Dec. 2004.

[3] M. Mourad, H. Salem, and B. Ridha. Analysis of frequency offsets and phase noise effects on an OFDM 802.11 g transceiver. *IJCSNS International Journal of Computer Science and Network Security*, 7:87–91, April 2007.

[4] P. Shia-Sheng. WLAN IEEE802.11a Transceiver, Algorithm, Architecture and Simulation Results. Agilent Technologies document, `http://cp.literature.agilent.com/litweb/pdf/5989-8895EN.pdf`.

[5] Fuqin Xiong and Monty Andro. The Effect of Doppler Frequency Shift, Frequency Offset of the Local Oscillators, and Phase Noise on the Performance of Coherent OFDM Receivers. NASA document, `http://gltrs.grc.nasa.gov/cgi-bin/GLTRS/browse.pl?2001/TM-2001-210595.html`.