híradástechnika

VOLUME LVI.

2001/9

Selected papers

Theoretical background

Mobile systems

Traffic routing

Scientific Association for Infocommunications

Tartalom

ELMÉLETI HÁTTÉR

MOBIL RENDSZEREK

FORGALOMIRÁNYÍTÁS

Editorial Office
Communications and IT Sciences Association
HTE Budapest, Kossuth Lajos tér 6-8.
Phone: 00 36 353 1027 • Fax: 00 36 353 0451
e-mail: hte@mtesz.hu

Articles can be sent also to the following address
BME Microwave Communication Department
Budapest, Goldmann Gy. tér 3.
Phone: 00 36 463 1559 • Fax: 00 36 463 3289
e-mail: zombory@mht.bme.hu

Subscription
Communications and IT Sciences Association
HTE Budapest, Kossuth Lajos tér 6-8.
Phone: 00 36 353 1027 • Fax: 00 36 353 0451
e-mail: hte@mtesz.hu

Subscription rates in 2001
For Hungarian business customers HUF 30,000 per year (including VAT), for Hungarian residential customers
HUF 6000 per year (including VAT). For foreign subscribers 12 issues 150 USD, single copies 15 USD.

www.hte.hu

Publisher: MÁRIA MÁTÉ

Design by: Kocsis és Szabó Kft.

HU ISSN 0018-2028

Preface

In our second issue, mainly students, doctorands and their mentors report on the major achievements of their research. Surveying such reports, we may see that currently, the research conducted in the High Speed Network Laboratories, Budapest University of Technology and Economics (BME-HSNL) is focused on improving Internet-based telecommunications. We can read interesting results of the management of such networks, on expanding the scope of services and of quality improvement. They endeavor to provide the users with a quality equal to the usual quality of the circuit switched networks; however, they also want to derive the economic benefits of the new solutions.

According to the main profile of HSNL unifying the groups interested from different professorates, they study different problems of Internet-based fixed and mobile networks. Both theoretical and practical achievements are utilized by telecommunications carriers and the manufacturing industry. In order to promote this process, universities and users have established an organization denominated Inter-University Telecommunications and IT Center (ETIK). This meeting point facilitates fast communication of needs to research workers; and the parties interested can have direct access to the results.

This contact is also favorable to the universities – and to the students working for ETIK. Namely, users support ETIK, this way making the staff of ETIK financially motivated. In many cases, support also covers the procurement of explorers. As an outcome of the cooperation, a number of research themes topical worldwide are dealt with. In the course of the work, significant theoretical achievements, such as the interesting analogy between biology and certain physical phenomena, are revealed.

Several themes included in this issue prove that achievements of research conducted at universities may evoke the interest widely. Such achievement are likely to result in products in the coming 2 to 3 years. However, a problem comes up: will these themes studied be topical at the time when these future engineers will have become leaders of research groups? Experiences show that in electronics and information technology, all the knowledge acquired by the young people at the university become obsolete in 10 to 15 years. Engineers have accepted that they need to refresh their science on and on. On the other hand, fast development has the risk that this period of 10 to 15 years reduces to 5 to 7 years, i.e. a student in his fourth year who continues studying for his Ph. D. will have to study again with his newly acquired doctorate.

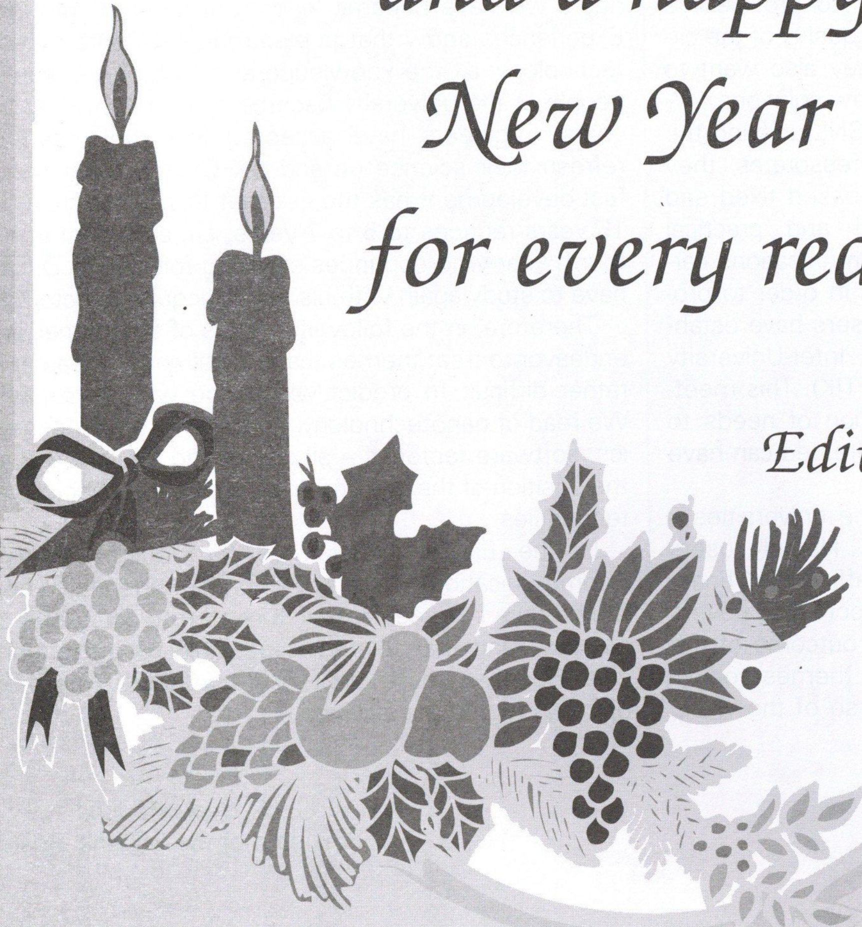
Therefore, in the following issues of the journal, we endeavor to treat themes that are still rough ideas. It is rather difficult to predict which one will be realized. We read of nanotechnology, photonics, micromechanics, software factories – all competing for taking over the position of the currently predominant technological tendencies.

In the English version of the journal entitled "Communications", we endeavor to moderately keep the balance between research related to actualities of our days and that related to possible future tendencies. Hopefully, our readers will contribute with their opinions to find this balance.

Dr. György Lajtha
President of the Editorial Board

We wish
a merry Christmas
and a happy
New Year
for every reader

Editorial Board



Global Positioning System after turn off Selective Availability (SA)

BENCE TAKÁCS

PhD student, Budapest University of Technology and Economics, Department of Surveying and Geodesy

According to an investigation at the early 1990 [1] the expected growth of GPS users between 1990 and 2000 in the area of civil aviation is about 140 times, in the area of land traffic 60 times, in the area of civil maritime 65 times. At the same time the expected growth of military users is only 12 times. At the beginning of May 2000 President Clinton declared turning off Selective Availability. The accuracy of real-time GPS positioning became ten times better, and the experiences show that generally it is possible to reach some meters accuracy. Turning off SA probably caused significantly larger interest for GPS units by civilian sphere (tourists, alpinists, rally drivers, sailors, sky troopers etc). How accurate is the real-time GPS positioning? In this paper the accuracy of stand-alone GPS positioning without SA is investigated using several receivers.

Introduction: brief overview of GPS

The NAVSTAR GPS (NAVigation System with Time and Ranging Global Positioning System) is a satellite-based navigation system providing precise three-dimensional position, velocity, and time information to suitable equipped users. The all-weather system is continuously world-wide available. GPS has been under development by the US Department of Defense (DoD) since 1973, and is a military system, with limited access to civilian users.

The satellites, considered as control points with known positions, are continuously moving in the space, but their movement can be described precisely, so their position at any epoch can be computed.

Positioning means measuring the range from the receiver to the satellites. From the geometrical point of view three non coplanar ranges are sufficient. Practically a fourth observation is necessary because the receiver clock is generally not synchronized with the satellite clock, so besides the three unknown coordinates of the receiver the clock offset is to be taken into account as an unknown parameter. For this reason, the distance measured to the satellite is not the "true" range, but it is called "pseudorange".

Determination of the receiver's unknown position is achieved in the following steps

- measuring sufficient number (at least four) of pseudoranges
- computing the position of the satellites in a suitable reference system
- computing the position of the receiver, using pseudoranges we measured

Each satellite has high performance frequency standards. Two carrier frequencies in the L-band are coherently derived from the fundamental 10.23 MHz frequency

L1: 154 x 10.23 MHz = 1575.42 MHz (the wavelength is ≈ 19.05 cm)

L2: 120 x 10.23 MHz = 1227.60 MHz (the wavelength is ≈ 24.45 cm)

Each satellite transmits signals on both frequencies. The carriers are modulated by pseudorandom noise (PRN) codes. These are sequences of binary digits (zeros and ones) which appear to have random character, but which can be identified unequivocally. Two different codes are in use, the P-code (precise or protected) and the C/A-code (clear or coarse/acquisition). To determine the signal propagation time, the user has the copy of the code sequence in his receiver. This code sequence is shifted in time step by step and correlated with the received code signal until maximum correlation is achieved. The necessary shift is a measure of the signal travel time between the satellite and the receiver antennas. This technique can be explained as code measurement. According to the structure of the codes the theoretical precision of the code measurement is 3 m with C/A-code, and 0.3 m with P-code.

For precise geodetic applications the pseudoranges have to be derived from carrier phase measurements because of the much better resolution. A carrier phase measurement is achieved by reconstructing the original signal (pure sinusoidal wave). The receiver has to know the modulating codes. There are some observation techniques, where it is possible to reconstruct the signal without knowing the codes, but of course with limited accuracy.

Carrier phase measurements are affected by an ambiguity term, that is, by an unknown number of integer wavelengths between the satellite and the receiver antenna. The initial ambiguity has to be determined with appropriate techniques; this is one of the most demanding problems in the GPS data processing. The carrier wavelength is about 20 centimeter wavelength, so the pseudoranges might be determined by phase measurement with 2 mm accuracy.

Besides the code and phase measurement their combinations might also be used by special algorithms called phase smoothed code measurements.

Each satellite broadcasts so called navigation message on both frequencies. Its most important parts are:

- clock corrections: to transform the satellite time into GPS time system
- orbital parameters and corrections: to compute the position of the satellites in the reference system of GPS

The reference system is an ellipsoid of revolution. Its size and shape are fixed by international conventions. The immediate result of a satellite positioning is a set of X, Y, Z-values in the WGS-84 (World Geodetic System, 1984) which can be converted into ellipsoidal latitude, longitude and height (or vice versa) using mathematical formulas.

There are several methods of positioning:

- Using single receiver, this is the stand-alone or absolute positioning. Its result is the current set of X, Y, Z coordinates of the receiver's antenna
- Using two receivers, this is the relative positioning. Its result is the vector (or coordinate differences) between the two receivers. Generally one of the receivers (base station) is on a known point
- If during the observation the other receiver (rover) does not move, it is the case of static relative positioning, if it moves kinematic relative positioning
- In real-time positioning results are available "in situ"; with post-processing method the results are computed later

The relative positioning is more accurate than the stand-alone one, because from the observations at the base stations the systematic errors can be modeled. The static positioning is more accurate than kinematic one, because of the lot of redundant measurements. Increasing the observation time, the impact of random errors can be reduced.

The positioning are affected by several errors (the list is not complete at all):

- The errors of orbits and clocks are systematic errors
- The ionospheric delay means a systematic error too, its impact can be eliminated using dual frequency receivers. If using single frequency receiver the delay can be modeled through the ionospheric parameters transmitted among navigation messages
- The tropospheric delay can be modeled in the processing software
- Signal interferences with itself caused by multiple refraction results, is a systematic error
- The drift of the antenna's phase center, the background noise in the atmosphere and the internal noise of the receiver can cause random errors. The so called satellite geometry increases the impact of random errors, the increasing factor can be described via the quantity of Dilution of Precision (DOP). It depends on the relative position of the receiver and the tracked satellite
- Gaps in phase data can be caused by loss of lock during tracking to a satellite. Cycle slip means some missing integer number of cycles from continuous phase measurment. Generally the processing software can detect and repair these errors

According to the purpose of application there are geodetic and navigational receivers. Navigation must be a real-time method; surveying uses generally a relative- static method. According to the different applications there are differences between the receivers too: the navigational units have a fast processor, the geodetic ones have large capacity in data storing.

Fixed tests achived a very accurate navigation for only C/A code pseudorange positioning, so the initiator (DoD) decided to deny civilian users full use of the system. This limitation was the Selective Availability (SA), which means the strong degradation (in 4-5 order in magnitude) of the stability of the atomic clocks on the board of the satellites. One can imagine it, as an artificial dithering of the frequency. According to the initiator's announcement [3] in the consequence of Selective Availability the errors are less then 100 meters in horizontal position and less than 156 meters in height at 95% probability.

It should be noted, that SA degrades only the standalone, real-time positioning (i.e. navigation). With post-processing or with relative positioning the impact of SA can be eliminated.

Selective Availability was introduced in March 1990; it is interesting, that during the Gulf-war its application has been suspended for three months.

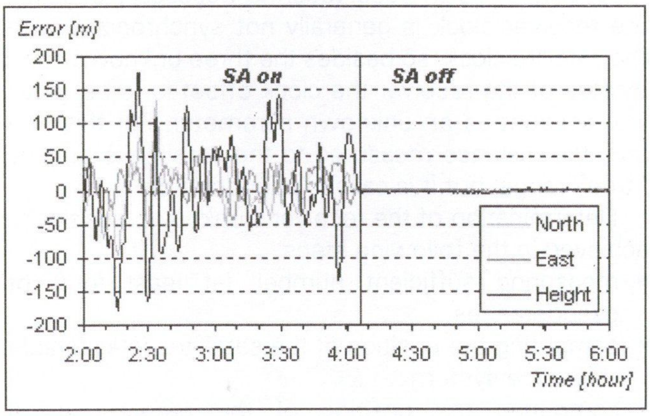


Figure 1. Errors of stand-alone positions calculated from the measurements of IGS permanent station Penc (Hungary), at early morning on 2 May 2000, during turning off SA

The initiators have confirmed several times, that the degradation is only temporary. The President of US announced in 1996, that the degradation will be terminated within ten years, and in May 2000 announced the decision to stop degrading GPS accuracy [5]. The result can be seen on Fig. 1.

What could be the main causes of turning off SA:

- Priority of economical interests: the analysis expects a very strong growth of GPS users especially in the field of civilian navigation.
- Defending market share: according to the plans the European Community will operate an own GPS, called Galileo. It promises more services than NAVSTAR GPS.

Beside SA another limitation should be noted, which assures the security of GPS signals against falsification, it is called Anti-Spoofing (A-S). It means a transformation of P-code into an unknown Y-code via an encrypting W-code, implementation was in the beginning of 1994; the signal protection is still alive.

It should be mentioned that even with active SA and A-S using a special a hardware element (Auxiliary Output Chip, AOC) one can reach full information of GPS signals. This element – it is available only with permission of DoD – is to be built into each channel of the receiver.

As it was mentioned before, the "official" accuracy is around 10 meters, but our experiences show a more favorable trend. The accuracy was investigated both in static and kinematic case, the main results are presented in this paper.

Static measurements

Measurements during 24 hours period were carried out on a known point with recording the coordinates calculated by the receiver. The "true" and "measured" positions were compared, so the differences are considered as true errors. For demonstrating the accuracy the distributionfunction of the errors was used (Fig. 2.), the main results are shown in the Table 1.

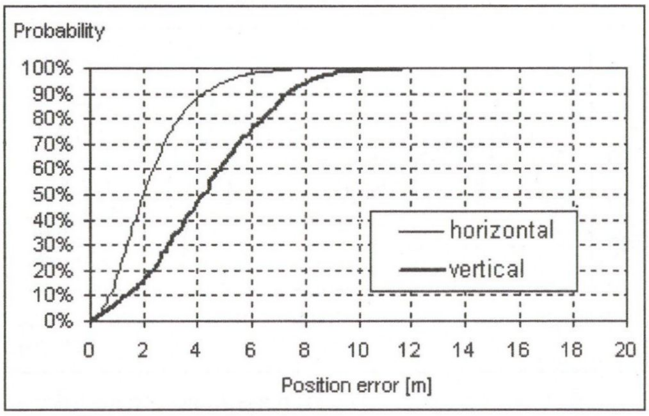


Figure 2. Error distribution function

Receiver	Horizontal error [m]			Vertical error [m]		
	68.3% (1σ)	95.4% (2σ)	99.7% (3σ)	68.3% (1σ)	95.4% (2σ)	99.7% (3σ)
Trimble 4700	2.1	4.3	9.7	5.3	9.2	15.1
Trimble 4000 SSE	2.8	5.3	6.8	3.0	7.0	9.0
Trimble 4000 SST	3.8	6.7	9.3	6.0	11.0	16.0
Pathfinder CBS	2.7	4.4	7.7	3.1	7.4	10.0
Topcon Turbo-G1	2.6	4.7	8.4	10.9	15.1	20.0
Garmin eMap	2.7	5.2	7.8	4.2	7.2	10.8

Table 1. Result of static measurements with several receivers

The test was run with three different geodetic receivers (first three raws in the table) and with three handheld, low-cost receivers (second three rows). The accuracy of horizontal positions is around 5 meter; the vertical component is around 9 meter on two sigma level. It is very impressive, that the geodetic receivers and the low-cost ones can be characterized with nearly the same accuracy. Differences between the receivers are mainly in the vertical components. The TOPCON receiver has large errors in the vertical component, compared to the other ones. Later investigation has shown that the software of TOPCON does not take into account the delay of ionosphere, so the vertical component has a more or less constant error of 5 – 10 meters (Fig. 3.).

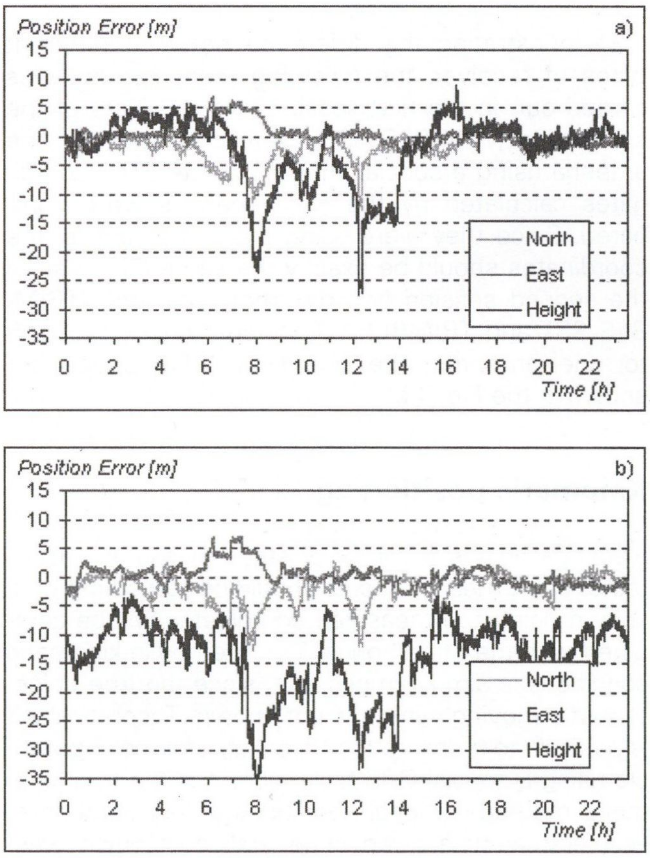


Figure 3. Position errors of stand-alone positioning a) with; b) without modeling the atmospheric delay

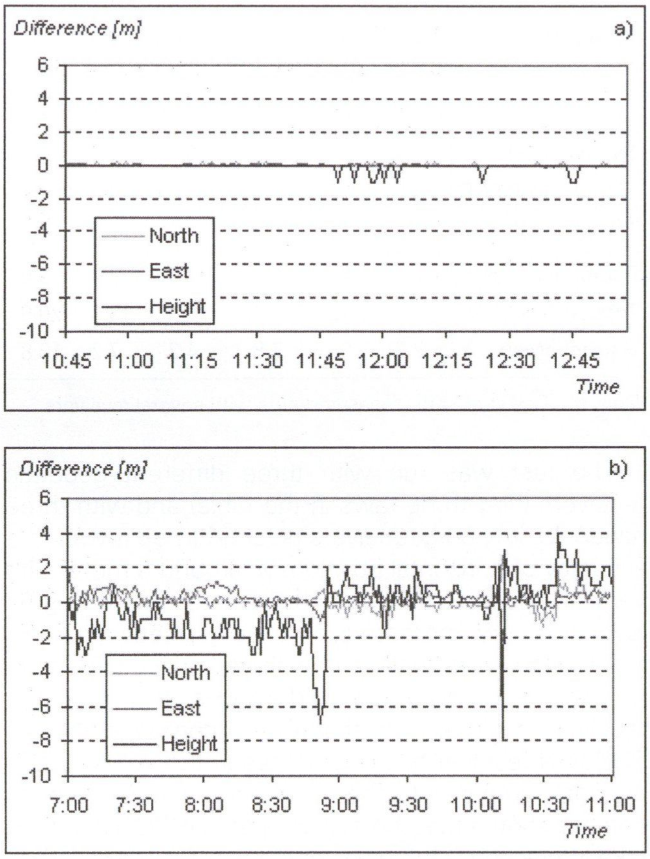


Figure 4. Two receivers connected to the same antenna a) same type of receivers (TRIMBLE SSE), b) different type of receivers (TRIMBLE SST and SSE)

Demonstrating the difference between different types of receiver, the following measurement was carried out: in the first session two receivers of the same type (TRIMBLE SSE) were connected to one antenna using a special antenna splitter. The coordinates calculated by the two receivers were compared. Since they were using the same signals, the coordinates should be exactly the same (Fig. 4.a). In the second session two different receivers: (TRIMBLE SST and TRIMBLE SSE) were connected again to one antenna. The coordinate differences are shown in the Fig. 4.b.

Kinematic positioning

Investigating the accuracy of static measurements is rather easy: measurements should be carried out on a known point, the measured coordinates will be compared with the "true" ones. This method in kinematic conditions is almost impossible, since the true trajectory of a moving vehicle is not known. Theoretically it is possible to measure the trajectory of a moving vehicle using a special GPS technique; it is the true kinematic method. In ideal conditions a few centimeter accuracy can be achived. In general conditions however the receiver satellite lock is interrupted too often by different obstacles.

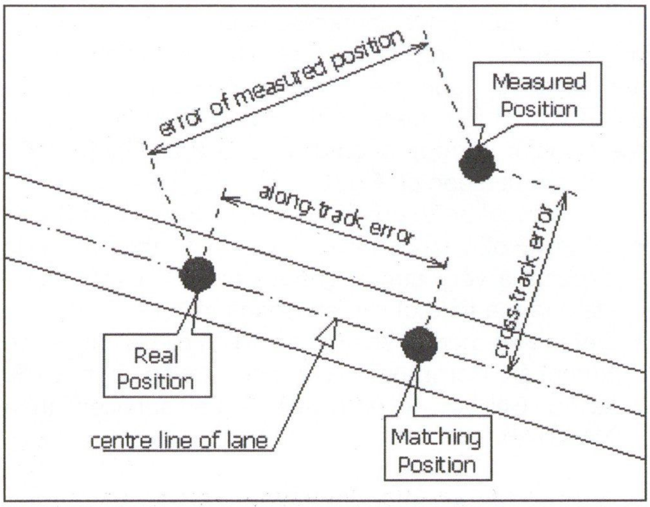


Figure 5. Cross-track error, along-track error and true error of a measured position

An effective method to estimate accuracy is, to compare the trajectory computed by a receiver placed on the top of a moving car with a "theoretical" one. If the road was surveyed before, and the data are available in a coherent database, the "theoretical" trajectory may be considered the known center line of the lanes. Calculating the perpendicular distances of the measured positions from the "theoretical" trajectory one can estimate the accuracy of kinematic positioning. Of course this data is not the position error; it is only the cross-track error, since it does not contain the component along the trajectory. (Fig. 5.)

The experiences show, that the accuracy of static measurement is more favourable than in kinematic case. The main reasons may be as follows:

- In the kinematic case due to the different obstacles the configuration of received satellite changes often
- The receiver software probably uses a Kalman-filter algorithm [6]. It means the current position is an optimal weighted mean of the predicted and the measured one. Supposing 80-100 km/h velocity and 1-5 second sampling interval, the prediction (and its covariance) should be rather uncertain.

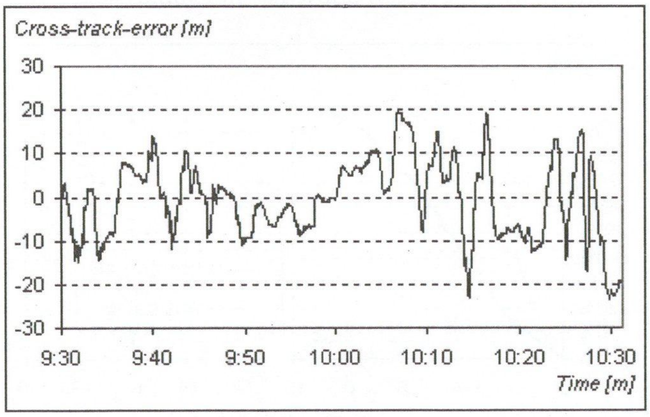


Figure 6. Cross-track errors at during measurement on the highway M3 (Hungary)

Another significant difference between static and kinematic measurements is that the errors of the static measurements are more or less constant even within a longer period (10-30 minutes), but in the kinematic case the cross-track errors may fluctuate very rapidly (Fig. 6).

Differential GPS

The effect of Selective Availability was able to be eliminated before May 2000 using so called differential corrections. The main idea of the method is the following: if two receivers track simultaneously to the same satellite, the difference of result is free of most systematic errors, including SA. In practical realization one receiver (base station) works on a known point. Since the coordinates of the satellites are known, the range between the receiver and the satellite can be calculated. Comparing this calculated value to the measured one, the previously mentioned differential corrections can be determined. Correcting the measured range at the rover receiver with these differential corrections, the position of the rover receiver can be determined with the accuracy of some meters. We need a communication channel to transfer the corrections in (near) real-time. The accuracy strongly depends on the latency of corrections. Latency means the time necessary to transfer corrections. Currently (September 2001) in Hungary differential corrections are available receiving special RDS services or special messages from geosynchronous satellites.

When the SA was turned on, the latency of the differential corrections was the critical point, since the corrections were changing rapidly (Fig. 7.). In Fig. 1. we saw, that the most important result in turning off SA was, that the error of stand-alone positioning decreased from 100 m level into a few meters level. This means, several applications do not need differential corrections, since 5-10 meters accuracy can be reached without them. It is important to note, that for some applications (especially the precise and reliable navigation) the accuracy of stand-alone positioning is not sufficient, so the differential corrections will remain of importance.

Another important result of turning of SA is, that the latency is no more critical, since the corrections can be considered constant in a short arc.

Conclusion

Test measurement demonstrated that with turning off Selective Availability, the accuracy of a stand-alone GPS receiver position is better than 5 meters in horizontal sense, and 9 meters in height at two sigma level. As the accuracy of stand-alone positioning is concerned, there is no real difference between the geodetic and low-cost handheld receivers. Further important experience is, that some receivers do not use enough finel models to correct some systematic errors (see ionospheric delay at TOPCON Turbo-G1).

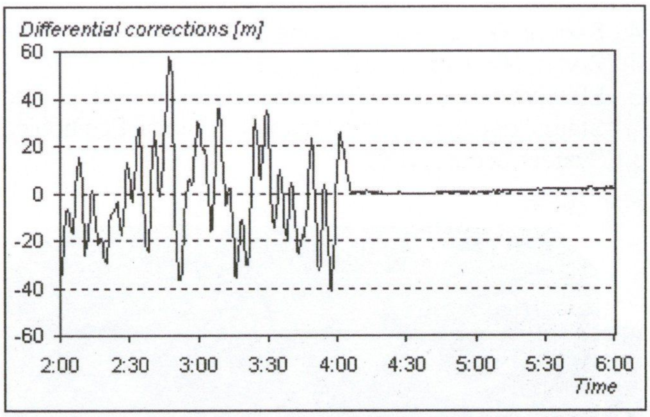


Figure 7. The errors of satellite-receiver pseudoranges or – with opposite sign – the differential corrections at the permanent station Penc, on 2. May 2000 before and after turning off SA.

The accuracy of kinematic measurements was also investigated. We found significantly larger errors, than in static case. We estimated the accuracy by the so called cross-track errors; these values can often reach 10 or 15 meters. Further important difference between static and kinematic case, that the "static" position errors are nearly constant for a longer period, while the fluctuations of the "kinematic" error can be very fast. It is caused probably by the rapid changes in satellite geometry.

Another important consequence of turning off SA is that the rate of differential corrections is rather slow, so the transmission time of these corrections will no more critical. It is very important to emphasize, that in the future the differential technique remains necessary in accurate and reliable navigation applications.

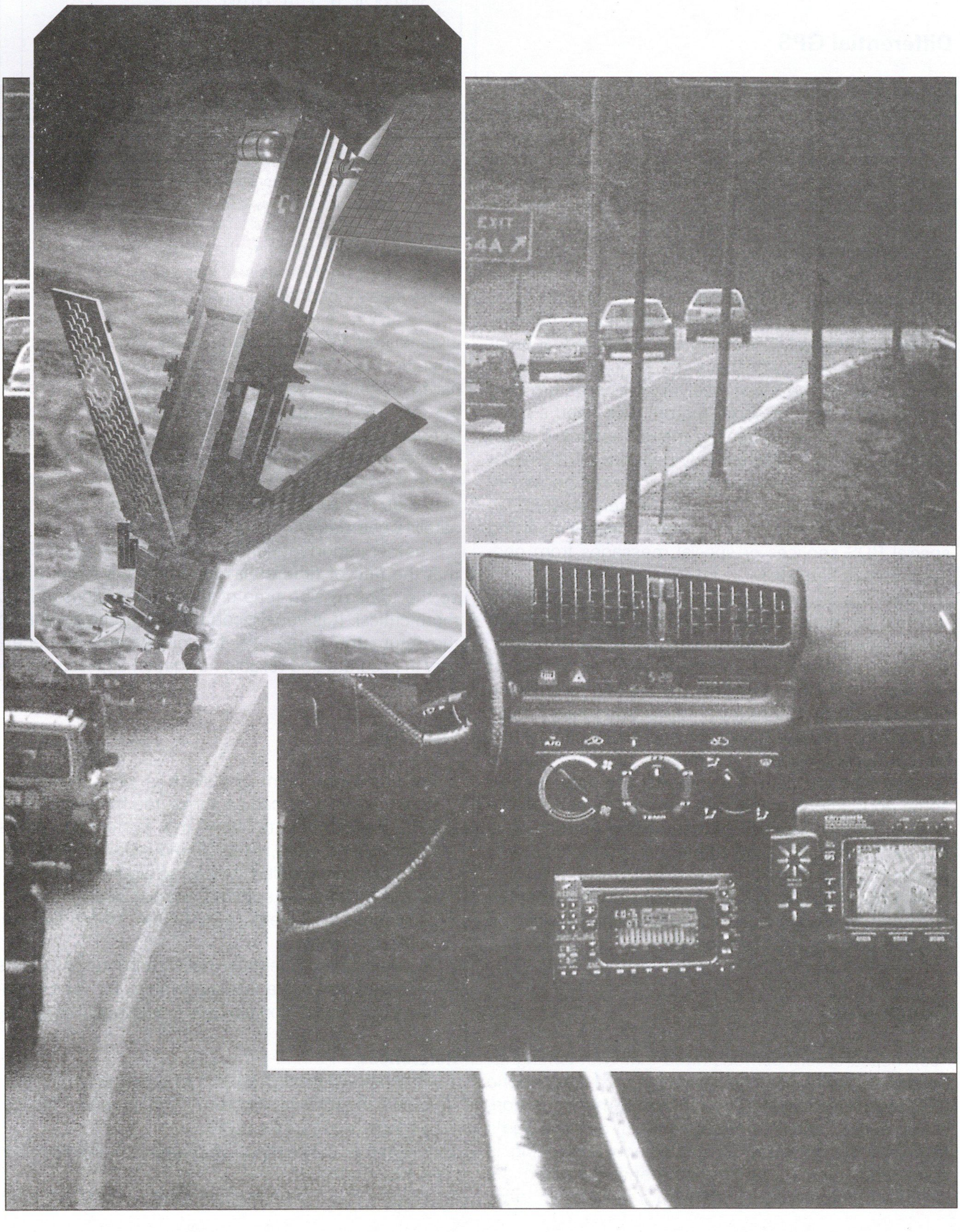
Outlook

1. For theoretical point of view it is very interesting, how the positions can be computed form the "raw" GPS measurements, how the systematic errors (atmospheric delay, satellite and receiver clock offsets) can be modeled. Since the algorithms applied by the commercial software are not public, it would be useful to develop a software under General Public License.
2. To investigating kinematic measurements it would be necessary to build a suitable system for vehicle ztajevtory determination which is independent of GPS.

References

1. Hofmann-Wellenhof B., H. Lichtenegger, J. Collins.: Global Positioning System. Theory and Practice. Springer-Verlag, Wien, 1997.
2. Krauter A.: Surveying (in Hungarian). Műegyetem Kiado, Budapest, 2001.
3. Langley, R. B.: Dilution of Precision. GPS World. 1999.

4. Seeber G.: Satellite Geodesy. Walter de Gruyter, Berlin, New York, 1993.
5. Statement by the President regarding he United States' decision to stop degrading Global Positioning System accuracy, 2000.
6. Takács B.: Application of Kalman-filter in modern Satellite Geodesy (in Hungarian). Magyar Távközlés. 2000.



Genetic Algorithms for Parameter Identification of the Classical Scalar Preisach Hysteresis Model

MIKLÓS KUCZMANN, AMÁLIA IVÁNYI

Budapest University of Technology and Economics
Department of Electromagnetic Theory

Abstract. The classical Preisach model and its modifications are one of the most generally applied simulation methods to model the behaviour of magnetic materials, to describe hysteresis phenomena. According to the theory of Weiss, the classical Preisach model assumes that the ferromagnetic materials consist of many elementary interacting domains, and each of them can be represented by a rectangular elementary hysteresis loop. The fundamental concepts of the Preisach model is that different domains have some distribution, which can be described by a distribution function, also called Preisach Kernel, can be approximated by a Gaussian type probability distribution function with four variables. A genetic algorithm has been applied to determine the parameters of the classical scalar Preisach hysteresis model. Hysteresis loops, measured in the rolling and in the transverse directions have been applied for the identification process, then the hysteresis characteristics simulated by the Preisach model and curves from measurements are compared and plotted in figures. Errors of the prediction are also analysed.

Keywords: anizotropy, genetic algorithms, hysteresis characteristics, magnetic materials, Preisach model.

Introduction

The simulation of hysteresis characteristics of magnetic materials is very important in wide range of Computer Aided Design (CAD) software applications and in electromagnetic field calculation tasks. Hysteresis characteristics of magnetic materials can be described by a nonlinear, multivalued relation between the magnetic field intensity $H(t)$ and the magnetization $M(t)$. Many available approaches and hypothesis have been developed since the last period of magnetic research, as the Preisach model, the Jiles-Atherton model, the Stoner-Wohlfarth model and so on [1,2,3,7,8]. There are some parameters of these models must be identified and fitted to the measured hysteresis loops.

Genetic Algorithms

Genetic Algorithms (GAs) are stochastic global search and optimization methods based on the mechanics of natural selection and genetic processes of biological organisms. The main idea of these algorithms is to modify the tentative solutions of a design or an optimisation problem, called population and to produce new solutions, called off springs. While a real optimum, a given error or a given generation number is not reached, the generation loop is still on work [4,5].

GAs are capable of searching global optimum in a multidimensional space, can be found more effectively, however traditional search and optimisation methods may stuck on sub optimum, furthermore calculation of the gradient of objective function is not necessary. Due to their robust and general nature, GAs have been successfully applied to many optimisation problems.

Aim of optimization is to find the global minimum $\mathbf{x}_{opt}$ of an objective function $f(\mathbf{x})$ with N variable

$$\mathbf{x}_{opt} = \arg \min_{\mathbf{x}} f(\mathbf{x}). \tag{1}$$

Real GAs can be applied when $\mathbf{x}_{opt} \in \Re^N$. After initialization of the generation some genetic operations (selection, recombination, mutation, reinsertion) must be applied to find a better generation that is a better solution.

Construction of the applied GA

A GA based on the distance, the radius and the diameter conception of the current generation has been applied. This kind of algorithms has more fast convergence speed than other general GAs [5,6].

At first, some definitions are given. Denote the individual of the current generation with the highest fitness ξ. The individual with the farthest distance from the best individual ξ is denoted by Σ_f, and the two individuals with the farthest distance of any other two individuals are defined as Σ_1 and Σ_2, moreover the distance between these individuals is the diameter of the actual population, $D=d_{\Sigma_1,\Sigma_2}$. The distance between the individuals ξ and Σ_f is the radius of the actual population, $r=d_{\xi,\Sigma_f}$. The distance between two individuals η and $\mathbf{v}$ is defined by the Euclid distance,

$$d_{\boldsymbol{\eta},\mathbf{v}} = \sqrt{\sum_{i=1}^{N}\left(c_{\boldsymbol{\eta}}^{(i)} - c_{\mathbf{v}}^{(i)}\right)^2}, \tag{2}$$

where $c_\eta^{(i)}$ is the i^{th} variable, that is the i^{th} chromosome in individuals. The so-called genetic stock is defined as the group of these four individuals, $\mathbf{G}(k) = [\xi\ \Sigma_f\ \Sigma_1\ \Sigma_2]^T$. It may be different for every generation.

Fitness function $F(\mathbf{x})=\Psi(f(\mathbf{x}))$ is defined as ranking of individuals

$$F(\mathbf{x}_i)=1-\frac{f(\mathbf{x}_i)}{\max\limits_j\left(f(\mathbf{x}_j)\right)}, \tag{3}$$

where $i, j=1,\ldots, N_{ind}$ and N_{ind} denotes the number of individuals of the population.

The population in the next generation is performed by the crossover and the mutation operations. Parents for crossover can be chosen by the selection operation. The so-called retention rate (selection rate) in the k^{th} generation is defined as

$$r_s(k) = \frac{3}{2} - \frac{r}{D}, \tag{4}$$

where r is the radius and D is the diameter of the current population [5]. According to the fitness value, all individuals must be sorted by descendant order, and then a random number p_i must be generated in the interval $[0,1]$ for every individual. The selection rule is defined as follows, if $p_i > r_s$, then put the individual into the group of parents. Afterwards, the individuals ξ and Σ_f also must be put into the selected individuals. If the radius r is large, more diverse individuals are selected into the next generation, otherwise if the radius is small, fast global optimization is guaranteed. It is similar to the roulette-wheel selection.

Off springs in the next generation is generated by the crossover operation between selected parents. The individuals ξ and Σ_f, moreover Σ_1 and Σ_2 perform intermediate crossover. And the other selected parents also perform intermediate crossover, that is

$$\begin{cases} \eta_o=\alpha\eta_p+(1-\alpha)\mathbf{v}_p, \\ \mathbf{v}_o=\alpha\mathbf{v}_p+(1-\alpha)\eta_p \end{cases} \tag{5}$$

where η_p and $\mathbf{v}_p$ are the parents and η_o and $\mathbf{v}_o$ are the off springs, and α is a real number, which is different for every chromosomes, selected randomly from the interval $[0,1]$.

Mutation can increase the diversity of the population according to the mutation rate, r_m which is a small real number in the interval $[0.001,0.01]$. A chromosome of the individual is modified randomly.

The new individuals that are the off springs are reinserted into the population in the next generation.

The block diagram of this GA can be seen in Fig.1.

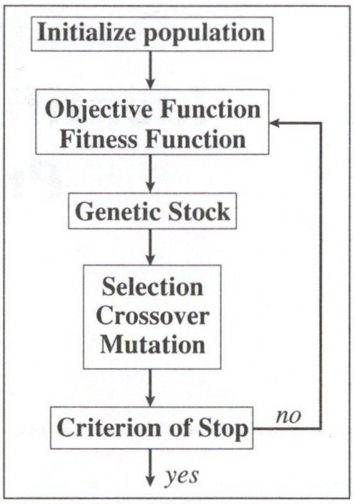


Fig.1. Block diagram of applied genetic algorithm

There are some test functions to analyze the ability of GAs to find the global optimum as the Rastrigin function, the Rosenbrock function and so [4]. The Rastrigin test function with two variables is defined as

$$f_t(x_1,x_2)=20+\left(x_1^2-10\cos(2\pi x_1)\right)+ \\ +\left(x_2^2-10\cos(2\pi x_2)\right) \tag{6}$$

and plotted in Fig.2, and the variations of population with 50 individuals during iteration are drawn and the fast convergence speed is illustrated in Fig.3. The global minimum of this function is $\mathbf{x}_{opt}=[0\ \ 0]$.

The classical Preisach model

According to the theory of Weiss, the classical Preisach model assumes that the ferromagnetic materials consist of many elementary interacting domains, and each of them can be represented by a rectangular elementary hysteresis loop [1]. The fundamental concepts of the Preisach model is that different domains have some distribution of switching fields h_a and h_b, which can be described by a distribution function $P(h_a,h_b)$, also called Preisach

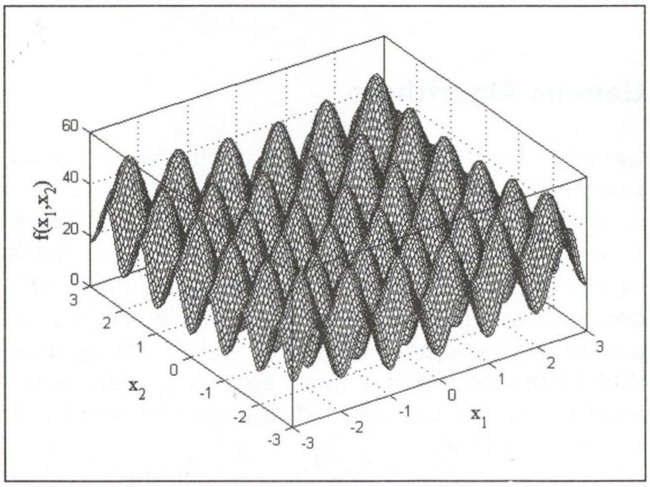


Fig. 2. The Rastrigin function

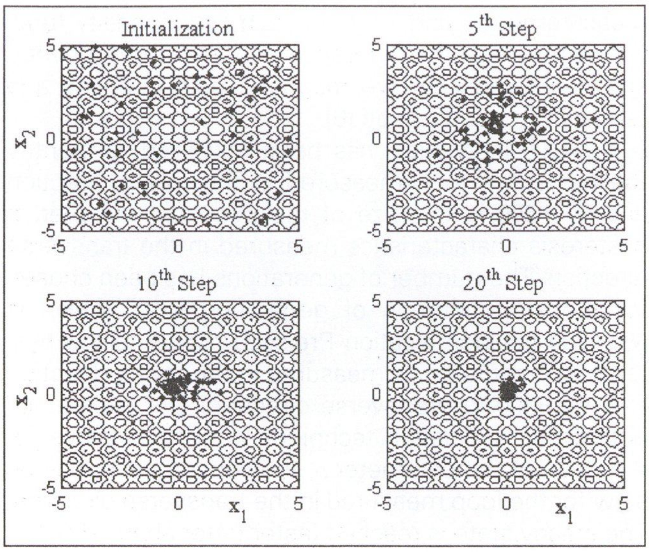


Fig. 3. Variation of population

Kernel, and the magnetization $M(t)$ can be calculated as

$$M(t)=\iint_{h_a \geq h_b} P(h_a,h_b)\cdot\gamma(h_a,h_b)\cdot H(t)\,dh_a dh_b\,, \tag{7}$$

where $\gamma(h_a, h_b)\cdot H(t)$ is the elementary hysteresis operator. Two-dimensional Gaussian distribution functions can be used for analytical approximation of the distribution function. The following Gaussian distribution has been used in the implemented Preisach model

$$P(h_a,h_b)=\begin{cases}\exp\left[-\dfrac{(h_a-h_b-c)^2}{10^a}-\dfrac{(h_a+h_b-d)^2}{10^b}\right], & h_a+h_b\leq 0,\\[2ex] \exp\left[-\dfrac{(h_a-h_b-c)^2}{10^a}-\dfrac{(h_a+h_b+d)^2}{10^b}\right], & h_a+h_b>0\end{cases} \tag{8}$$

where parameters a, b, c and d can be used to fit the given major loop, moreover $h_a\in[-1,1]$, $h_b\in[-1,1]$ [3]. An example for the Gaussian distribution function and hysteresis characteristics generated by the Preisach model are plotted in Fig.4. Here a=–0.667, b=–0.762, c=0 and d=0.

The measurement of hysteresis curves

The identification of Preisach model is realized on measured data, plotted in Fig.5 and Fig.6 performed at the Bioelectricity and Magnetism Laboratory, Vienna University of Technology. The measurements have been accomplished on a single sheet tester consisting of a U shaped vertical yoke. The laser scribed, grain-oriented 27ZDKH95 specimen with thickness 0.27 mm is produced by Nippon Steel. The dimensions of the specimen are 500×500 mm^2. The anisotropic material is separately exposed to sinusoidal waveform of an alternating flux density, first in the rolling direction and in the transverse direction afterwards. The measured data consist of 512 $H-B$ pairs in every curve. Three measured hysteresis loops are analyzed [2,8].

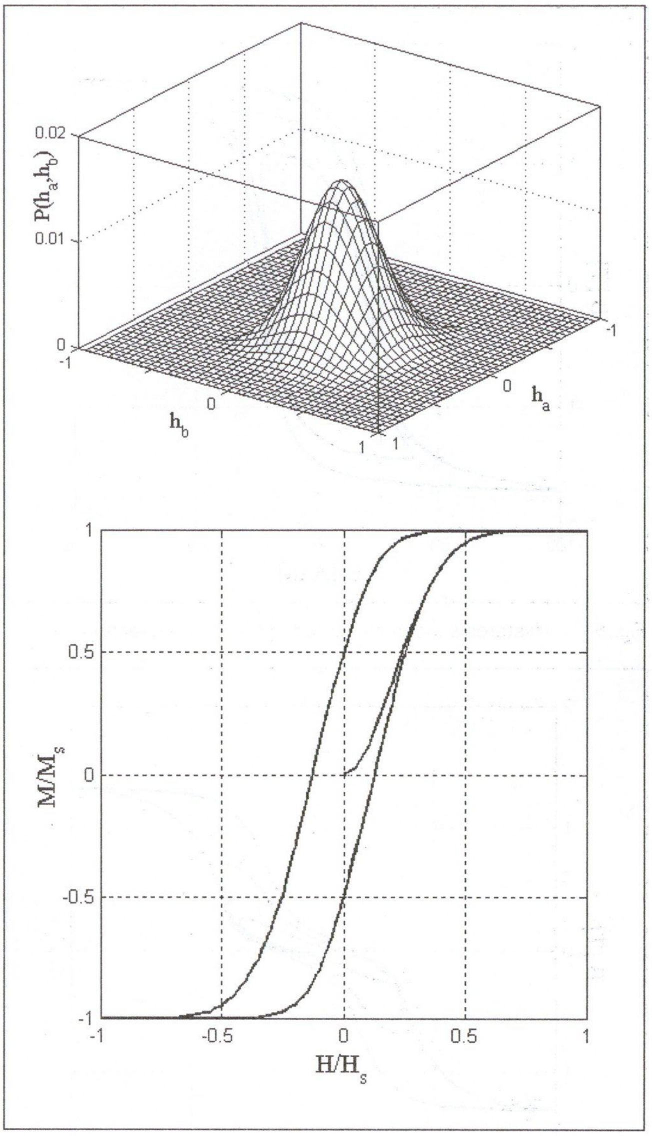


Fig. 4. Gaussian distribution function and the appropriate hysteresis characteristics

Parameter identification using GA

The objective function is determined as the difference between simulated and measured main loops (3rd loops in Fig.5 and Fig. 6), that is

$$f_{Obj}=\frac{1}{N}\sqrt{\sum_{i=1}^{n}(M_{Pr,i}-M_{Meas,i})^2+f_P}, \tag{9}$$

where N is the number of $H-M$ pairs, M_{Pr} is the normalized magnetization simulated by the Preisach model, M_{Meas} is the normalized magnetization from

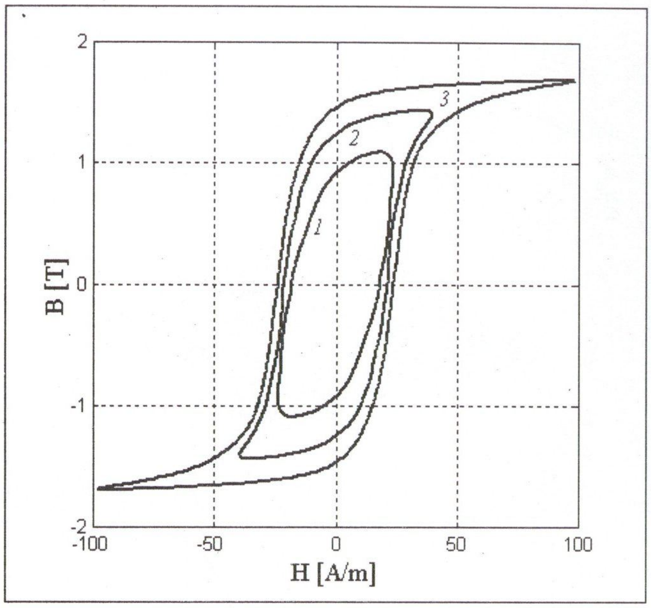


Fig. 5. Hysteresis loops measured in the rolling direction

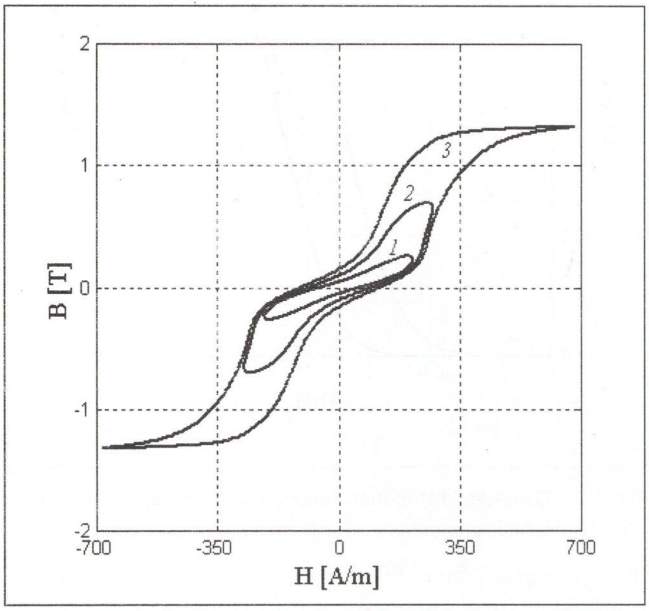


Fig. 6. Hysteresis loops measured in the transverse direction

measurements, and $f_P=f_P(\Delta H_c,\Delta M_r)$ is a penalty function to minimize the difference between the simulated and measured coercive magnetic field intensity and remanent magnetization [6].

N_{ind}=100 individuals has been initialized to identify the hysteresis loop measured in the rolling direction and N_{ind}=200 is the size of the population to predict hysteresis characteristics measured in the transverse direction. The number of generations has been chosen for the stop criterion of generation loop, which is N_{gen}=200 for identification Preisach model to the hysteresis characteristics measured in the rolling direction and N_{gen}=300 for transverse direction. Our experience is that this simulation technique is very sensitive for the value of the parameter b, the convergence may be slow for the loop measured in the transverse direction. The steady state is reached faster (after about 150 iteration step) when the parameters for the hysteresis curve measured in the rolling direction are developed. Steady state is reached after 220 steps when hysteresis curve measured in the transverse direction is identified.

The values of parameters a, b, c and d after generation loop has stopped are as follows, a=–0.84683, b=–0.54231, c=–0.42961 and d=–0.94599 in the rolling direction, and a=–0.20796, b=–1.07260, c=–0.61348 and d=–0.60119 in the transverse direction. The result of parameters is the individual with the highest fitness, which is the best individual. Comparisons between hysteresis curves simulated by the identified Preisach model and measurements are plotted in Fig.7 and Fig.8.

The simulation error between measured and simulated magnetic flux densities can be expressed as

$$\Delta B = 100\left(B_{Meas} - B_{Pr}\right)/B_s \qquad (10)$$

where B_{Meas} is the measured, B_{Pr} is the simulated magnetic flux density and B_S denotes the saturation magnetic flux density of the 3rd measured hysteresis loop. Maximum value of this difference is reached at the coercive field and not more than 25%.

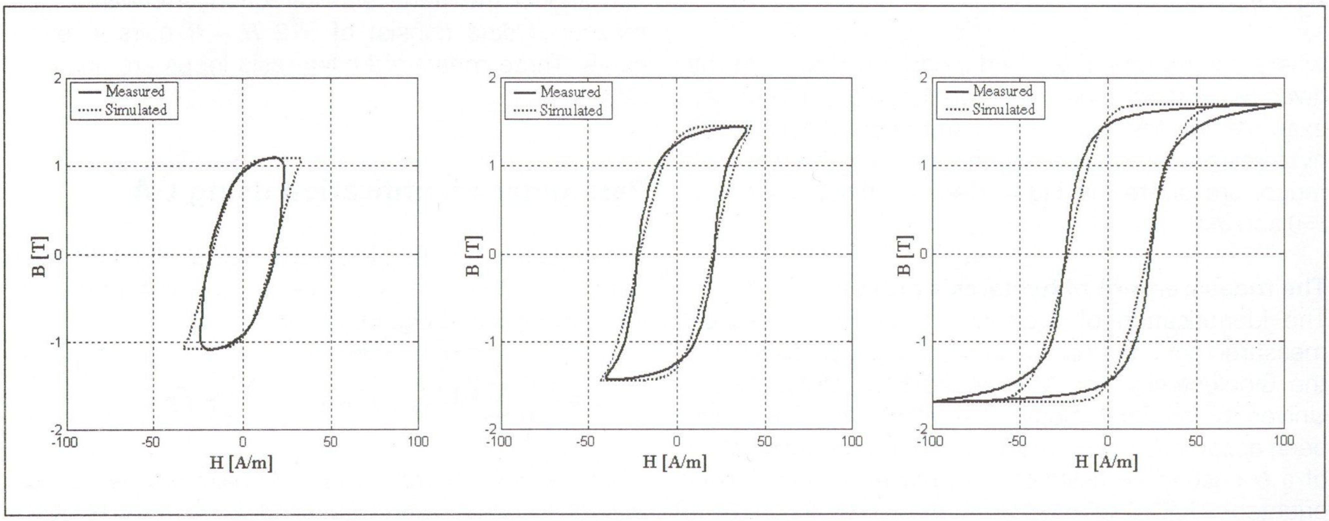


Fig. 7. Comparison between simulation and measurements in the rolling direction

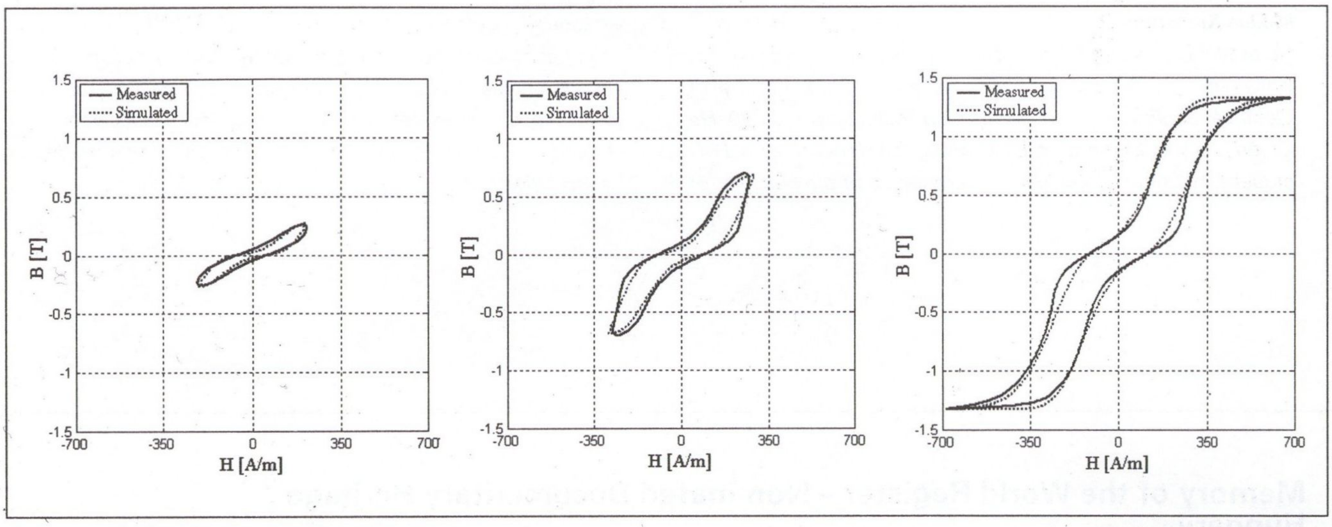


Fig. 8. Comparison between simulation and measurements in the transverse direction

The simulation error between measured and simulated magnetic field intensities can be expressed as

$$\Delta H = 100\left(H_{Meas} - H_{Pr}\right)/H_S \ , \tag{11}$$

where H_{Meas} is the measured, H_{Pr} is the simulated magnetic field intensity and H_S is the magnetic field intensity in saturation state of the 3rd measured hysteresis curve. It is the inverse hysteresis characteristics, which is important when field equations are solved by the vector potential $\boldsymbol{A}$. The magnetic flux density can be expressed as $\boldsymbol{B}=\nabla\times\boldsymbol{A}$, and $\boldsymbol{B}=\mu_0(\boldsymbol{H}+\boldsymbol{M})$, so the magnetic field intensity $\boldsymbol{H}$ and magnetization $\boldsymbol{M}$ can be predicted by the inverse characteristics [2]. Maximum of this difference is reached at saturation state and not more than 20%.

To compare the differences between measurements and simulation, the hysteresis losses w from the enclosed area of the characteristics are also determined as

$$w = \oint H dB \ . \tag{12}$$

The differences between the 3rd loops are less than 10%, which is important, because the so-called excess losses that are depending on the magnetic domain width, on the microstructural inhomogeneity and so. It can be associated to an eddy current loss, but cannot be approached by the Maxwell equations, and its value is about 10% [2].

Conclusions

A GA based on the distance conception of the actual generation has been used to determine the parameters of the classical Preisach hysteresis model. Hysteresis characteristics simulated by the identified model and measurements are compared and the errors are also expressed and shown in figures. There is a good agreement between prediction and measurements.

This kind of GAs has a fast convergence ability, can be applied for many fields of engineering applications, and identification problems.

Acknowledgement. The research work is sponsored by the Hungarian Scientific Research Fund, OTKA 2001, Pr. No.: T 029778.

References

1. A. Ivanyi, Hysteresis Models in Electromagnetic Computation, Akadémia Kiadó, Budapest, 1997.
2. A. Ivanyi, Magnetic Field Computation with R-functions, Akadémia Kiadó, Budapest, 1998.
3. J. Füzi, Parameter Identification in Preisach Model to Fit Major Loop Data, in Applied Electromagnetics and Computational Technology, vol.11, IOS Press, 1997, pp. 77-82.
4. B. Lantos, Genetic Algorithms (in Hungarian), Budapest University of Technology and Economics, Department of Control Engineering and Information Technology, 1995.
5. H. Liang, J.Z. Cui, Application of Conception of Distance for the Genetic Algorithm, Computational Engineering Using Metaphors from Nature, ed.by B.H.V. Topping, Civil-Comp Press, Edinburgh, Scotland, 2000, pp. 99-103.
6. M. Kuczmann, A. Iványi, Genetic Algorithms for Parameter Identification in Hysteresis Models, IEEE International Workshop on Intelligent Signal Processing, Budapest, Hungary, May 24-25, 2001, pp.87-92.
7. Zs. Szabó, A. Iványi, Simulation of Vectorial Hysteresis in Anizotropic Materials (in Hungarian), Híradástechnika, Budapest, Hungary, Vol. 1, 1999/9, pp.15-38.
8. J. Füzi, E. Helerea, D. Oltenau, A. Iványi, H. Pfützner, Experimental Verification of a Preisach-Type Model of Magnetic Hysteresis, Studies in Applied Electromagnetics and Mechanics, Vol. 13, Non-linear Electromagnetic Systems, 8th ISEM Conference Braunschweig, IOS Press, 1997, pp. 479-482.

Miklós Kuczmann

He obtained diploma in electrical engineering at the Budapest University of Technology and Economics at the Faculty of Electrical Engineering and Information Technology in 2000. He joined the Department of Electromagnetic Theory as a PhD student. His research field is the simulation of the behavior of magnetic materials applying artificial neural networks and soft computing methods, electromagnetic field calculation and nondestructive testing. He got the price of SIEMENS for diploma thesis. Member of the Scientific Association for Infocommunications and the Hungarian Electrotechnical Association.

Memory of the World Register – Nominated Documentary Heritage
Hungary
Kalman Tihanyi's 1926 Patent Application "Radioskop"

The television system, which in the wake of the publication of Kalman Tihanyi's French and British patents of 1928 priority gave new direction to television development, is recognized by historiography as one the great inventions of the 20th century. This invention, the last of the three „evolutionary leaps" discernible within the developmental history of television, made possible its technical realization and industrial mass-production.

The documentary heritage is the first description by the inventor of his television system, and the only existing complete collection of documents representing the Hungarian patent applications he filed in 1926 under the name "Radioskop". The significance of this document, then, resides in the fact that it is here the inventor first laid out the fundaments of modern television featuring a fully electronic television transmitting and receiving system and introducing, among many novel features, the operating principle of accumulation and "storage" of electrical Charges throughout each scansion cycle.

Thoughts on feasibility of code-breaking

Dr. József Dénes

mathematician, retired scientific researcher

The word cryptology is derived from two Greek words: kryptos = hidden, logos = word. A plaintext can be converted into a ciphertext through encryption. With the applied key in hand the legitimate receiver can convert the ciphertext into plaintext. Illegitimate receivers are called cryptanalysts. The illegitimate activity is called cryptanalysis. (There are numerous cryptology handbooks, such as [12].)

Voltaire (1694–1778), an outstanding thinker of the French enlightenment said the following on this subject:

„Those who fib to be able to read an encrypted letter without any help and without knowing its subject are charlatans even more than those who fib to understand a language that they never learned before."

Voltaire was unaware of the cryptanalytic efforts of Viète (1540–1603), a French mathematician hundred years before. Voltaire's misconception had a long impact over the next few centuries. Recently I held a presentation to executives responsible for bank security and the head of one of the largest banks said, in the spirit of Voltaire, that it is easy to achieve security, only enciphering is needed.

Another misconception was stated by Stimson (1867–1950) (from 1929 to 1930 Foreign Secretary, from 1911 to 1913 and from 1940 to 1945 Defense Secretary of the USA): "Gentlemen do not read others' letters." He said this in 1929 when he ordered closure of the USA's Cipher Bureau, Black Chamber. Later the USA had to pay a high price for this error.

The NSA (National Security Agency), established in 1954. the USA's cipher organization which operates the largest computer capacity and employs the most mathematicians within a single organization in the world. [1].

The British cipher organization, GCHQ (Government Communications Headquarters) is somewhat smaller than the NSA [15].

The security of an encryption system is difficult to judge. Babbage (1792–1871), a British mathematician and cryptanalyst said: "As a basic rule we can say that no one should try to design a secure encryption code who has not broken yet a difficult code."

The view of Babbage arises again 150 years later when Snow, an NSA expert says: "I would never trust an encryption algorithm designed by someone who has not spent earlier a lot of time on cryptanalysis." Then he continued: "I observed that almost nobody meets this criterion in the business world of encryption. This is what makes our job at NSA easier."

Past and present

Cryptography and cryptanalysis are mostly done by mathematicians. This statement is substantiated by an arbitrary selection of renowned cryptanalysts from the 15th to the 19th century:

L. B. Alberti (1404–1472), G. Cardano (1501–1576), Viète (1540–1603), J. Wallis (1616–1703), G. W. Leibniz (1646–1716), L. Euler (1707–1783), C. B. Babbage (1792–1871), W. S. Jevons (1835–1882). Although this list is far from being complete, it should be noted that each of these cryptanalysts were mathematicians too. The same can be seen in a list of 20th century cryptanalysts, similarly far from being complete:

A. A. Albert, L. D. Calimahos, G. Cullmann, C. Deavours, L. D. Dodgson alias Lewis Carroll, W. F. Friedmann, J. Good, G. Hammel, E. Hüttenkhain, R. Kochendörfer, G. Köthe, S. Kullback, W. Kunze, E. Pannwitz, A. Paschke, M. Rejewski, H. Rohrbach, R. Schauffler, G. J. Simmons, A. Sinkov, K. Stein, A. Turing, W. H. Tutte, M. de Vries, G. Welchman, H. Ziggalski.

A reference to the interrelation between cryptography and mathematics is made by a well-known statement of A. A. Albert: "Abstract cryptography is nothing else than abstract mathematics."

The security of encryption is difficult to judge even in mathematical terms. One thing is sure, only one of the encryption systems developed so far is mathematically demonstrated to be unbreakable, the one-time pad method.

Vernam (1890–1960) was working with AT&T (American Telephone and Telegraph Company) with responsibility for research on telecopy. This led him to the concept of automated encryption. He invented the stream cipher machine [13] which used the one-time pad algorithm. [14]. A random number is added to the binary plaintext according to the Boolean algebra rules to generate the ciphertext.

Note: The difference between physical random numbers and pseudorandom numbers is that for the former certain parameters of a random physical process are defined, while for the latter the pseudorandom numbers are derived with a mathematical algorithm.

Boole addition: 0+1=1, 1+0=1, 0+0=0, 1+1=0				
Plain text:	10110101	Solution:	Chipertext:	10011000
Key:	+ 00101101		Key:	+ 00101101
Chipertext:	10011000		Plain text:	10110101

The Venona project – How was it possible to break under the VENONA project the one-time pad algorithm used by the Soviets from 1939 to 1957? [1] (In the course of these efforts the USA had for a part of the period alliance with the Soviet Union.) Although the plaintexts derived from numerous Soviet ciphertext telegrams were published in [2], practically nothing was published about the method used for breaking the code.

One-time pad algorithms can also be broken when inappropriately used. The Soviets were using one-time pad algorithm for the encryption of high-security messages from the beginning of World War II. Since this method is theoretically unbreakable probably errors were made in the application of the encryption method. Now we try to analyze these errors.

The one-time pad algorithm replaces letters (or strings of letters) of the plaintext. To do this the original plaintext is converted to a stream that can be input to the communications channel. A physical random stream is used as key that is generated in advance independently of the plaintext, the letters used in the key stream are selected independently of each other so that each letter occurs with the same probability in the stream. The key stream is exchanged in advance between the transmitter and the receiver in an absolutely secure way. Then encryption is made by adding the key stream letters to the plaintext letters, independently of the given message, according to the Boolean addition table.

Probably the USA security services acquired the plaintext coding and the addition table since these were identical at all stations, they were not replaced periodicelly because they trusted in the security of coding. For us it is irrelevant from where they were acquired. It is known that in 1945 I. Gouzlenko, an encryption officer at the Soviet Union's embassy in Canada emigrated with the Soviet code and the current key streams. According to other assumptions American intelligence agents acquired the Soviet codes in Germany.

The one-time pad algorithm is theoretically unbreakable because each key is used only once then destroyed. This is inconvenient for the users: an extremely large number of random keys need to be generated, transmitted to the partner through an absolutely reliable channel, then stored absolutely securely. This technical problem resulted in a rough organizational error. It was ordered that the keys already used must not be destroyed, but later used again according to a defined rule. This way the command center degraded the theoretically unbreakable system to a breakable system.

First the cryptanalyst needs to find which messages were encrypted with the same key. When we have two ciphertexts generated with the same key we can deduct one from the other according to the applied addition table to generate the same differential text that would result from deducting one plaintext from another plaintext. This way the key plays no role. If we can generate from the differential text the two plaintexts our cryptanalysis efforts were successful.

A precondition to successful cryptanalysis is to be able to select from a large number of ciphertexts those generated with the same key. For this purpose we can use a very simple statistical test, the coincidence test proposed by Kasiski (1805–1881), Kerckhoffs (1883–1903) and Friedmann (1891–1969). In this test the two analyzed texts are checked letter by letter to count the places where the same characters are found. If the number of identical characters is sufficiently high then the differential text is judged to be a meaningful text, if the number of coinciding characters remains below a limit then the test suggests that different keys were used.

The test is very simple, but requires much time when manually done. Therefore a team was assigned to this task. The detected key repetitions were analyzed to find systematical rules. With their help key repetitions could be found very efficiently.

After World War II the Soviets performed encryption with electromechanical Vernam machines. This brought a new weakness into the system because American cryptanalysts could acquire direct information about the encryption streams through acoustical interception.

With the help of VENONA many Soviet spies could be unmasked (Klaus Fuchs, Harry Gold, David Greenglass, Theodore Hall, William Perl, Etel and Julius Rosenberg, Guy Burgess, Donald Maclean, Kim Philby, Harry D. White). The political protection of the information source (VENONA) was so strong that no information acquired with VENONA was raised as evidence in the Rosenberg couple's trial, not even at the retrial instituted by their sons. A one-time pad algorithm used by the Germans was broken by American cryptanalysts. [9]

ENIGMA was the cipher machine universally used by the German army in World War II. The ENIGMA cipher machine was commercially launched and patented in the 1920s. The first ENIGMA patent was registered in the USA in 1924 under patent No. 1657411.

In the same year the machine was presented at the World Post Exposition in Stockholm and could be tested, plaintext-ciphertext pairs could be generated with the machine. The acceptance of ENIGMA was reflected by the view of Colonel Figl, head of the Austrian cryptanalysis service published in 1926 stating that ENIGMA was an absolutely secure unbreakable machine. Figl's view was later (in 1942) shared by Safford, head of the American navy's cryptanalysis service.

The spice in the story is that in 1942 the British could break ENIGMA (without the knowledge of the allied USA).

Op-20-Q MEMORANDUM FOR OP-20 March 18, 1942

Subject: Security of information obtained from enemy communications.

1. During World War I (1914-1918), the British Admiralty was very successful in reading German naval messages and tracking German submarines by D/F. This was a well-guarded secret during the war. After the war, the British let down the bars of secrecy and told the world that they had done and how good they were. Apparently, it never occurred to the British that the Germans would profit by these revelations.

2. In World War II, the German ciphers and communication producers are such that the information obtainable by radio is substantially zero. With the exception of „weather codes" and certain other „minor systems" the only German naval messages which have been read have been the result of captures. Our prospects of ever breaking the German „Enigma" cipher machine are rather poor.

3. We are much more fortunately situated with regard to the Japanese Navy. Our solution of Japanese naval system began back in 1925. We are able to read most of the messages in the most important Japanese naval enciphering system and have completely solved one of the secondary systems. This is the result of sixteen years of unremitting effort along these lines. We are also getting considerable information by direction finding. We are faced with constant danger that news of our success will leak out, whereupon the Japanese will adopt steps which will nullify our efforts.

4. In 1938 and 1939, the Japanese Navy used a system which we have never succeeded in solving. They abandoned this system in 1940 and adopted a system which we can solve. The reason for abandoning the secure system is not known, but we surmise it was due its slowness and complexity. There is nothing that will stop their return to it if they find out that we are reading their messages.

5. What is even worse, they may adopt the German Navy cipher machine if news of our success leaks out. If this happens, our source of information will be reduced to direction finding and traffic analysis

6. This memorandum is submitted for the purpose of impressing upon all concerned that we must not compromise our one sure source of enemy information by a too wide dissemination of information.

Respectfully,
L. F. Safford
Captain, US Navy, Op-20-Q

Attack against ENIGMA was started by three Polish mathematicians. They were working in the Polish Cipher Bureau in the 1930s when they started solving ENIGMA. Soon they made substantial progress, but then fled from German occupation to France, then from the occupation of France to England.

The British cryptanalysis service perceived the great opportunity to solve ENIGMA. To help the solution they launched the greatest, best organized and most secret project of the time called ULTRA with the objective to solve ENIGMA and regularly supply information to the government. (At the end of the war 10,000 staff were working on ULTRA.) The objective could be reached, while various mathematicians were incorporated into the British cryptanalysis service, such as Turing.

Some conclusions that can be drawn from ULTRA are identified below because these can be applied to other systems too.

1. Solving an encryption system does not necessarily require trying out all potential keys. Detection, identification and machine-based processing of special features, so-called characteristics can bring results. The mechanical tools use for ULTRA were the so-called Bombe developed by the Polish, punched stencil-paper, and last but not least Colossus, the first digital computer of the world. (Colossus preceded the first electronic computers built in the USA.)
2. One of the keys to success is secrecy. The secrecy about ULTRA was so high (as I have mentioned) that one of the leading cryptanalysts of the allied USA Navy (Safford) declared in a report in 1942, when ENIGMA had already been solved, that he considered ENIGMA unbreakable. This is interesting for two obvious reasons. On the one hand Figl's view was shared still in 1942, on the other hand the secrecy of ULTRA was so high that even allied forces were not aware of the results.
3. When the security of an encryption system is judged and we declare that its solving requires, in addition to machine capacity available under given circumstances, some time then we must add that the first solution (called in technical jargon "breaking") and ongoing information supply are two different things. In the case of ULTRA breaking required years, while information supply was so fast that the German military commanders received ENIGMA messages practically at the same time when the British government received the deciphered messages.
4. The information acquired from cryptanalysis needs to be used in such a way that it has no detrimental impact on the source or the user (the activity of the cryptanalysts). A case that seems to be cruel reflects the importance given by the British military to keeping secrecy at any price. ULTRA obtained information about German plans to bomb Coventry. This was reported to Prime Minister Churchill. (It

should be mentioned here that ULTRA news were allowed to bypass the official channel.) Churchill decided that evacuation of the population would unmask ULTRA as news source so he did not approve evacuation. Churchill's decision took a heavy toll of human life, but hindered indirectly unmasking ULTRA, and this measure that seemed to be inhuman decisively contributed to the victory of the allied forces.

RSA is the algorithm most frequently used in public key cryptography [12], electronic commerce and bank services. This algorithm is named after its inventors River, Shamir and Adleman. The RSA algorithm is mathematically not unbreakable. Let us show an example of this, based on [11].

We demonstrate that the RSA algorithm can be broken when certain conditions are met. In the presented example we take two 30-digit prime numbers (p and q), compute their 60-digit product (r), use a 60-digit public key (e) and a 60-digit private key (d) '*M*' designates the plaintext, $M^e \equiv C$ $(mod\ r)$ the ciphertext. A cryptanalyst can know '*e*' and '*r*' from the public network, acquire '*C*' the ciphertext through tapping (or any other way). That is all the information available for retrieving '*M*' the plaintext.

First we present the major steps of encryption.

- Two 30-digit prime numbers are randomly selected independently of each other (p and q), then their product is computed (r) which is a maximum 60-digit number.
- A 60-digit exponent is randomly selected (e).
- The value of the product (r) in the $\varphi(r)=(p-1)(q-1)$ Euler function is computed, then it is used to compute the inverse(d) of 'e' according to modulus arithmetic.
- Then the message (or its beginning) is converted according to the system rules to a 60-digit '*M*' number and M is raised to the power of '*e*' using modulus r. This is the ciphertext '*C*'.

According to a Fermat (1601–1665) lemma if any number is multiplied with itself numerous times using a given modulus sooner or later the initial number will be obtained again. This is also true when the powers of a number are multiplied with itself. For the enciphering user the desirable case is that it should occur 'later', for the cryptanalyst it is descrable that is should occur 'sooner'. This is the situation in the above-mentioned example. We obtain the powers of C one after another. This requires only the knowledge of '*C*' and '*e*', without knowing '*d*'.

In practice we are encrypting repeatedly with overencryption. (This means that the ciphertext is raised to the power of '*e*' repeatedly.) This is continued until the plaintext is recovered. (The problem is that we have to recognize when we recover the plaintext. This is not complicated with human monitoring, but due to the potentially large number of repetitions the process needs to be automated.)

$$C_1 = C, C_2 = C_1^e \; mod \; r, \ldots, C_7 = C_6^e = C$$

This method shows in general that there are cases when overencryption produces result very soon. In the mentioned example recovery (of the plaintext without knowing the private key) is reached with six steps. It is important to know that with the use of RSA numerous similar problems may arise. These have to be taken into consideration by the system installation staff and users. We did not address the problem of randomly generating so large prime numbers. This is another typical source of error. (see [6], [12]).

p=	5862031427	1421210354	0772438083
q=	7976488510	8326808223	7297393713
r=	4675842632	8739231725	4879360844
	8514393251	3976539392	0565972179
e=	2271045762	1634362358	1376514176
	9315064549	8482805725	7408953697
Ed=1 mod φ (R)=	4675842632	8739231725	4879360843
	4675873313	4228520814	2496140384
D=	1132737643	4029650485	8021146249
	9965800024	6048577871	7422160801
M=	2008050013	0120080513	0120090301
	1200091420	0512120907	0514030518
$M^e \equiv C$=	5588998775	7849965411	4721338354
	9966344369	1263068475	835416031
$M^e \equiv C_1$=	5588998775	7849965411	4721338354
	9966344369	1263068475	835416031
C_2=	2237508320	7688556707	5596533921
	5205714326	6981783101	5567847029
C_3=	1255706821	9229988475	5285588845
	4913345628	8937978998	7617505740
C_4=	3919057992	8879931623	0065355244
	2837298453	0372725530	8484589194
C_5=	4432062157	4466035847	7637214037
	2485698933	3600141396	74016714
C_6=	2008050013	0120080513	0120090301
	1200091420	0512120907	0514030518
C_1=C_7=	5588998775	7849965411	4721338354
	9966344369	1263068475	835416031

This example shows (in addition to prime factoring) that even with a very large modulus RSA is vulnerable. There are also other parameter selections with which RSA offers poor protection.

We should draw some key conclusions from this simple example:

1. Trying out all keys is no general tool for cryptanalysis. This misconception was used by Gardner [5], when he was talking about the security of RSA that requires millions of years to break.
2. In general an encryption method should be secure even if we know the algorithm used for encryption.
3. The statistical tests used for cryptanalysis can be fully automated so the time needed for solving can be significantly reduced.
4. It is not correct statment that the only way of attacking RSA is prime factoring of the modulus. Simmons' example – reconstructed in this article – shows that RSA can be attacked other ways too.

Using Simmons' idea, Bolyai's result [8] and Schwartz' findings [10] a method could be achieved for attacking RSA that is not based on prime factoring, but detailed addressing this solution is beyond the limits of this article.

5. The security of RSA is weakened by the fact that official agencies use block ciphers rather than RSA (see a detailed discussion of block ciphers in [12]). The latest SKIPJACK algorithm is an example of this [7]. There are bad moduluses which do not depend on the length of the modulus [6], [12].

The future

The author (and presumably many others) trust in mathematically proven unbreakability. Accordingly he thinks that a modern version of one-time pad could have future.

The author has a double objective:

1. To create a modernized version of Vernam machines.

To demonstrate the most possible weaknesses of the RSA algorithm.

One-time pad requires a large number of physical random numbers. (Currently in the USA in one hour so many ciphertexts are generated as during the whole World War II.)

Delivery to the users of the keys needed for enciphering and their secure storage in the conventional way means an unsolvable problem for the designers. However there are very realistic ideas for the solution of this problem in the future. A random number generator located in a communications satellite could continuously emit a stream of physically random numbers to the Earth. Users A and B take a slice of this stream that is needed for enciphering. This requires synchronization between A and B. In the course of message transmission the used keys have to be destroyed (like now with one-time pad). This procedure can be applied for digital transmission (for transmission of text, sound, video, etc. signals). This procedure can be used also for mobile communications.

However attention must be paid also with this procedure to the errors that may be committed (for example those on which VENONA capitalized).

For example protection against acoustic tapping is replaced by the land terminal equipment protection against electronic radiation.

Against multiple encryption (e.g. DES = Data Encryption Standard) and a "hash" function (transformation of each plaintext to a defined fixed length /message digest/) there is a general very successful way of attack, „meet in the middle" (see [12]). One attack comes from the plaintext, while the other from the ciphertext, that is why this method is called „meet in the middle".

Attack can be hindered when the algebraic structure used for encryption is not commutative $(a+b\neq b+a)$ and not associative $((ab)c\neq a(bc))$ [4]. A practical implementation is shown in the patent application made by the author jointly with Messrs. Golomb and Welch to the USA's Patent Office.

Today algebraic structure based finite fields are used which are commutative and associative.

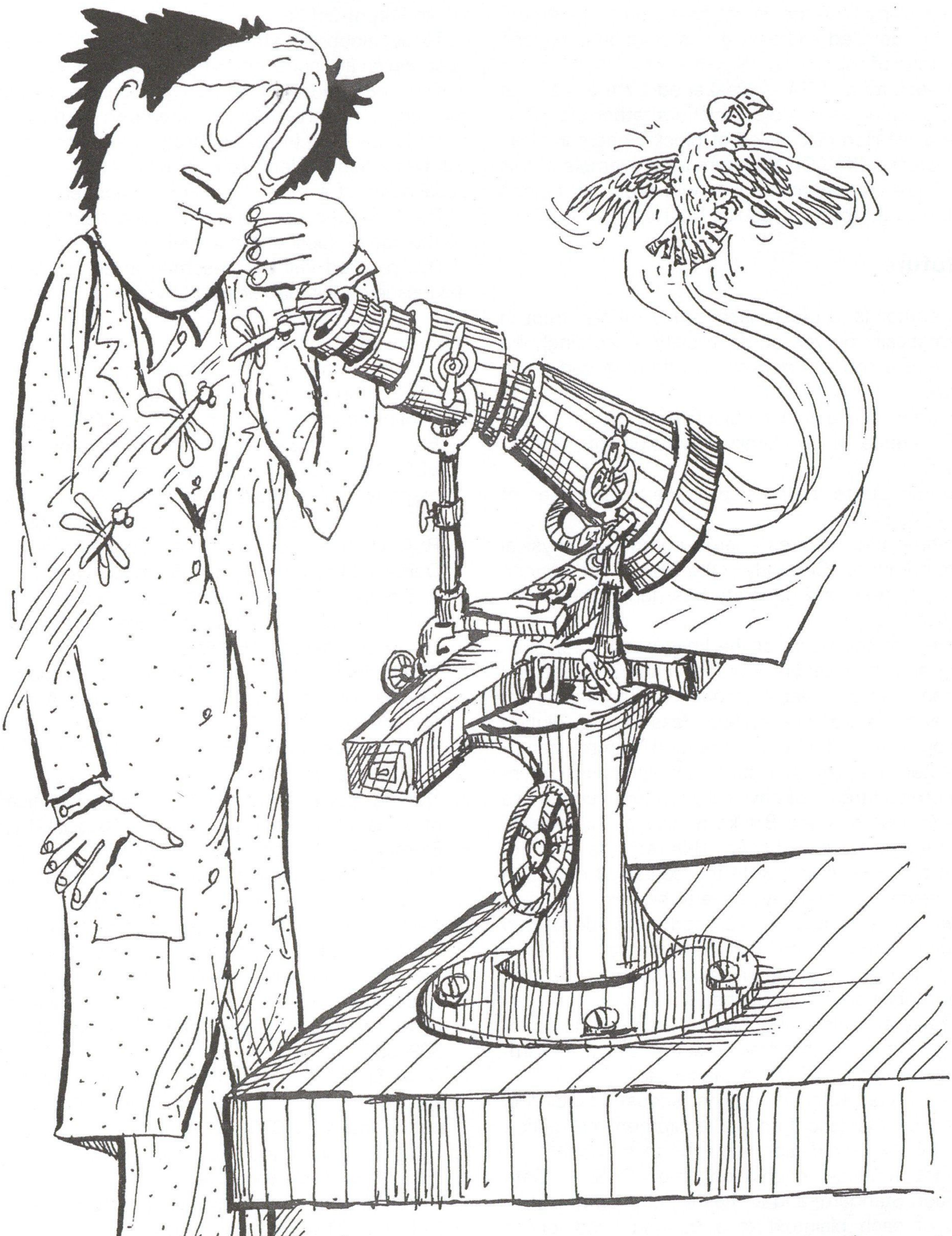
The word stenography has a greek origin, having the meaning a chipertext which seems to be meaningful but it is covering (masking) a confidental message. It can be named hidden text or hidden message. A quite usual name of it is also „subliminal channel".

The projected development in the next future will be the use of subliminal channel.

This method will be presented in an article in the next issue of 'Híradástechnika' by Tamás Dénes.

References

1. James Bamford: The Puzzle Palace: Inside the NSA, America's Most Secret Intelligence Organization. Penguin Books, New York, 1983
2. Robert Luis Benson, Michael Warner (eds.): VENONA. Soviet espionage and the American response 1939–1957. Aegean Park Press, 1996
3. J. Dénes, T. Dénes: On the connections between RSA cryptosystem and the Fibonacci numbers. Delivered for publication in Fibonacci Quarter.
4. J. Dénes, A. D. Keedwell: Some applications of non-associative algebraic systems in cryptology. Under publication in P.U.M.A.
5. M. Gardner: A new kind of cipher that would take millions of years to break. Scientific American, August 1977 120–124
6. S. W. Golomb: On factorization Jevons' number. Cryptologia, 20(1996) July No 3, 243–246
7. NSA Skipjack and KEA algorithm specification. http://carc.ncsl.nist.gov/encryption/skipjack-1.pdf
8. Elemér Kiss: Mathematical treasures in János Bolyai's manuscript legacy. Akadémia Kiadó, Budapest, Typotex Kft., Budapest, 1999
9. Cecil Philips: The American solution of a German one-time-pad cryptographic system. Cryptologia, 24, 2000, October 324–337
10. S. Schwartz: The role at semigroups in the elementary theory of numbers. Math. Slovacae, 31(1981) 369–395
11. G. J. Simmons: Cryptology: The mathematics of secure communications. The Mathematical Intelligencer, 1 (1979), 233–246
12. G. J. Simmons (ed.): Contemporary Cryptology. IEEE Press, New York 1992
13. Gilbert Vernam: Secret signaling system. 1.310.719 (July 22, 1919) American patent.
14. Gilbert Vernam: Cipher printing telegraph systems for secret wire and radio telegraphic communications. J. Am. Inst. Elec. Eng. 55/1926, 109–115
15. N. West: G.C.H.Q. CORET books, Hodder and Stoughton, London, 1987


DALLOS

Fuzzy monitoring of the safety-related critical processes

ING. MONIKA MOLNÁROVÁ
DOC. ING. JURAJ SPALEK, PHD.
University of Zilina, Faculty of Electrical Engineering,
Dept. of Information and Safety Systems
Slovak republic

Summary: In this paper model of the safety-related critical processes monitoring using fuzzy logic principles has been described. Output process variables are used in this model. Fuzzy state images of the monitored process are modeled by the composition of these variables. Method for setting of the hypotheses about the actual state of the process is discussed. The functions for safety controlling are defined by the set hypotheses.

Introduction

Safety-related critical process is a continuous of discrete technological process whose dysfunction effected by its own error or control error could cause damage to properties, health, human lives and environment [1]. System's tools for analysis and synthesis of control systems used in safety-related critical applications are similar to conventional but they are appended with tools for identification of the failure states and also with tools for affect analysis of the particular failure group, which is dominant from the safety point of view. Control precision and its safety rate depend on information quality about the actual state of the safety-related CP.

Safety-related critical process monitoring

Process monitoring is an action of gaining real images about the process selected features. The monitoring system is a complex of technological and software tools, which allow monitoring.

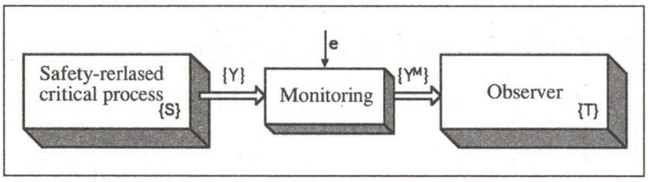


Fig. 1 Model of the safety-related critical process monitoring

Let safety-related critical process be a monitored object Fig. 1 with finite number of defined $\{S\}$. process monitoring can be described with transformation $M{:}Y\rightarrow Y^{M}$, $M^{\varepsilon}{:}Y\xrightarrow{\varepsilon}Y^{M^{\varepsilon}}$, where $Y\in\{Y\}$ are the output process variables of the monitored process, M is a correct transformation, executed by monitoring subsystem, M^{ε} is an incorrect transformation under interference influence ε. As a consequent, correct variable $Y\in\{Y\}$ is sensed by observer as an image $Y^{M^{\varepsilon}}\in\{Y\}$.

Exact regulation or exact control in closed loop can be achieved only following qualified monitoring, i.e. which provides real images about the controlled process state with adequate credibility. Firstly, state decomposition of the control system and controlled process is needed.

State decomposition of the process

Let $\{S\}$ be a state space of the safety-related critical process and contains E states according to Fig. 2:

$\{S\}=\left\{S^{K}\right\}\cup\left\{S^{\varepsilon}\right\}\cup\left\{S_{margin}\right\}$, where $\left\{S^{K}\right\}=(S_1, S_2, \ldots, S_k)$ is a subset of all correct (failure-free) states,

$\left\{S^{\varepsilon}\right\}=(S_{k+1}, S_{k+2}, \ldots, S_e)$ is a subset of all considered failure states,

$\left\{S_{margin}\right\}=(S_{e+1}, S_{e+2}, \ldots, S_E)$ is a subset of states irrelevant to the control function. Subset

$\left\{S^{K}\right\}$ includes states, which are from the control safety point of view critical (menace rate of the opera-

[1] *Ing. Monika Molnárová, Dept. of Information and Safety Systems, Faculty of Electrical Engineering, University of Zilina, Vel'ky Diel – NF, SK-01026 Zilina, Slovakia, E-mail: molnar@fel.utc.sk*

[2] *doc. Ing. Juraj Spalek, Ph.D., Dept. of Information and Safety Systems, Faculty of Electrical Engineering, University of Zilina, Vel'ky Diel -NF, SK-01026 Zilina, Slovakia, E-mail: spale@fel.utc.sk*

tional environment is not negligible) and states, which can be integrate to the group of safety, non-hazardous states. There is an assumption, that all states from the subset $\left\{S^{\varepsilon}\right\}$ are potentially dangerous. The control system is in charge to generate commands which minimize the risk.

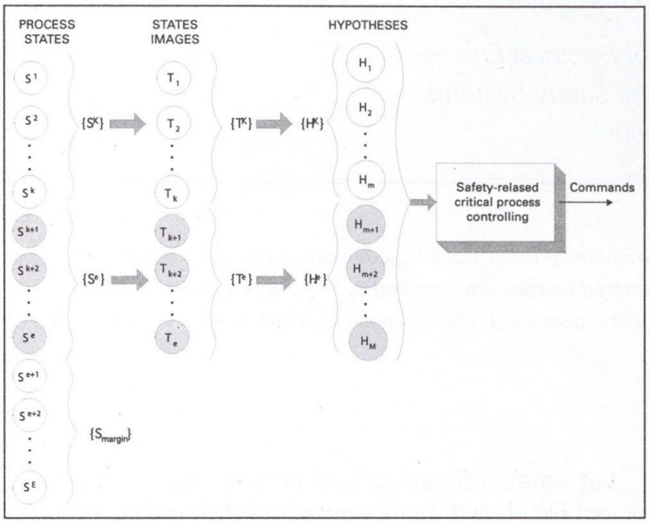


Fig. 2 Creation of the state-images and hypotheses setting

Composition of the fuzzy state-images

The control system which is in observer-role (Fig. 1) generates control variables based on obtained fuzzy state-images and corresponding control algorithm. For detailed behaviour description, finite set of state-images $\{T\}$ has to be defined. The elements of this set are images of the instantaneous state from set $\{S\}$ of the controlled process, obtained by transformation:

$$T(t){:}T \times Y(t), \tag{1}$$

Where T is an composition algorithm $Y(T) \to T(t)$. The elements of the set $\{Y\}$ are in practice represented by measurement of the physical variables of the controlled process. They are electrical variables. The set of state-images $\{T\}$ consists of subset T^K correct and subset T^{ε} incorrect images:

$\{T\}=\left\{T^K\right\} \cup \left\{T^{\varepsilon}\right\}$ where

$$\begin{aligned}
&\mathrm{T}^K(t){:}T \times Y^K(t) \Leftrightarrow T^K(t) \equiv S^K(t)\\
&\mathrm{T}^{\varepsilon}(t){:}T \times Y^{\varepsilon}(t) \Leftrightarrow T^{\varepsilon}(t) \neq S^K(t)\\
&\mathrm{T}^{\varepsilon}(t){:}T^{\varepsilon} \times Y^K(t) \Leftrightarrow T^{\varepsilon}(t) \neq S^K(t)\\
&\mathrm{T}^{\varepsilon}(t){:}T \times Y^{\varepsilon}(t) \Leftrightarrow T^{\varepsilon}(t) \equiv S^{\varepsilon}(t), \text{ ha } \alpha_{\mathrm{j}}^{\varepsilon} : S_j^{\varepsilon} \to Y_k^{\varepsilon}
\end{aligned} \tag{2}$$

The definition of the set of state-images $\{T\}$, which are observed by the observer, results in conditions, under which deformation of the actual state perception can occur. Observer has to provide to the control system qualified estimation of the actual process state. During the conventional monitoring, this estimation is discrete and can b incorrect. Fuzzy logic principles allow to quantify estimation credibility by state pseudo-partition (Fig. 3).

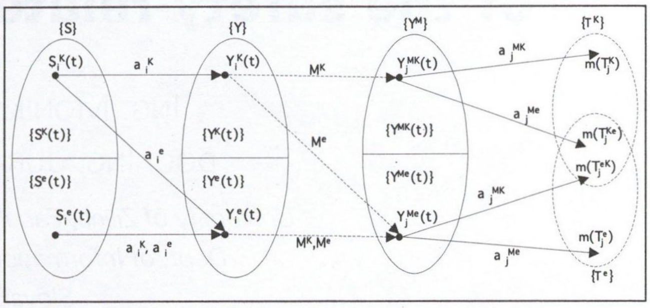


Fig. 3 Process monitoring by fuzzy state-images

Correct state $S_i^K(t)$ of the followed process is identified by the process variables either correctly $Y_i^K(t)=S_i^K(t) \times \alpha_i^K$ or incorrectly $Y_i^{\varepsilon}(t)=S_i^{K}(t) \times \alpha_i^{\varepsilon}$. First one could by evaluated by the observer with correct transformation M^K as a process variable

$Y_j^{MK}(t) \in \left\{Y^M\right\}$ or incorrect transformation M^{ε} as a process variable

$Y_j^{M\varepsilon}(t) \in \left\{Y^M\right\}$. At the same time α_i^K is a correct output function of the safety-related critical process,

$\alpha_i^{M^K}$ is a correct composition function of the monitoring system, through which observer creates state-image form the set $\{T\}$. In case of credible monitoring

$\alpha_j^K = \left(\alpha_j^{M^K}\right)^{-1}$. If observer receives also process variables correctly $M^K{:}Y_i^{M^K}(t) \to Y_j^{M^K}(t)$, then $T_j^K \equiv S_i^K$.

If either $\alpha_i = \alpha_i^{\varepsilon} \neq \alpha_i^K$ (as a consequent of safety-related critical process technical error) or $\alpha_j^M = \alpha^{M^{\varepsilon}} \neq \alpha^{M^K}$ (as a consequent of monitoring sensor error), then the result of the monitoring will be incorrect image from the set $\{T^{\varepsilon}\}$ and its credibility will be small. Monitoring based on fuzzy logic means that observer creates fuzzy images from the set of images $\{T\}$ of the real monitored process states $\{S\}$ following obtained process variables.

The credibility of the images T_j^K could be expressed with degree of membership $\mu_{T^K}\left(T_j^K\right)$ to correct fuzzy set of state-images $\left\{T^K\right\}$ or with degree of membership $\mu_{T^{\varepsilon}}\left(T_j^K\right)$ to failure fuzzy set of state-images $\left\{T^{\varepsilon}\right\}$.

Successful monitoring of the safety-related critical process requires solutions to the following problems:

a) to set the hypotheses relevant to particular kind of process risk and its control algorithm,

b) to quantify the degree of coincidence between the hypotheses and safety-related critical process real state,

c) to define threshold values of the hypotheses credibility accepted by control system.

Multicriterial control of the safety-related critical process differs from the conventional control mainly by algorithms based on set hypotheses about the process state relevant to particular kind of risk.

Hypotheses setting

Hypotheses are the set of statements about the instantaneous state of the controlled process. They are set to the fuzzy state-images which represent state of the controlled process relevant to control algorithm.

Let set M hypotheses about the instantaneous state of the monitored process with S states $M \leq E$. The hypotheses about the marginal states of the controlled process are not needful for the control algorithm, then $M \leq e$. About the k correct process state m hypotheses could be set, $m \leq k$. Similary, about the $(e-k)$ failure process state $(M-m)$ hypotheses could be set, $(M-m) \leq (e-k)$, see Fig. 2.

The observer creates the set of fuzzy state-images $\{T\}$ following process variables $\{Y\}=(y_1, y_2, \dots, y_p)$. Process variables are the systems of input variables which are used for creating the rules for state-images $T_1, T_2, \dots, T_e$ and coupled with integro-differential functions $\psi(y_1), \psi(y_2), \dots, \psi(y_p)$. compose a extended systems of input variables. Hypothesis Hh can be set only according to the assignment:

$$H_h : T_g, h = 1,2,\dots,M \text{ , } g = 1,2,\dots,e \text{ , where} \tag{3}$$

$$T_g : \left(y_1, y_2, \dots, y_p \middle| \psi(y_1), \psi(y_2), \dots, \psi(y_p)\right)_{T_g} \text{ ,}$$

where ψ is an integro-differential function for computing the gradient and median of the continuous process variables. e is a overall number of correct and failure process state, Fig. 2.

Assignment

$$T_g : \left(y_1, y_2, \dots, y_p \middle| \psi(y_1), \psi(y_2), \dots, \psi(y_p)\right)_{T_g} \text{ ,}$$

$g=1, 2, \dots, e$ is defined by fuzzy partition. Fuzzy partition creates domains divided into essential number of subspaces. Using fuzzy partition of the extended system of input variables, finite number of subspaces $h_a, a=1,2,\dots,A$ is formed:

$$\mathsf{h}_a = \left(\tilde{y}_1, \tilde{y}_2, \dots, \tilde{y}_p \middle| \tilde{\psi}(y_1), \tilde{\psi}(y_2), \dots, \tilde{\psi}(y_p)\right) \tag{4}$$

where

$$y_1^{a1} \leq \tilde{y}_1 \leq y_1^{a2} \text{ ; } y_2^{a1} \leq \tilde{y}_2 \leq y_2^{a2} \text{ ; } \dots \text{ ; } y_p^{a1} \leq \tilde{y}_p \leq y_p^{a2}$$

and

$$\psi^{a1}(y_1) \leq \tilde{\psi}(y_1) \leq \psi^{a2}(y_1);$$

$$\psi^{a1}(y_2) \leq \tilde{\psi}(y_2) \leq \psi^{a2}(y_2); \dots;$$

$$\psi^{a1}(y_p) \leq \tilde{\psi}(y_p) \leq \psi^{a2}(y_p).$$

Domains $\aleph_b$, $b=1, 2, \dots, B$; $B \leq A$ are developed by combination of subspaces see Fig. 4:

$$\aleph_b = \bigcup_{i=a_1^b}^{a_2^b} \mathsf{h}_i \text{ , kde } a_1^1 > a_2^1; \; a_1^1, a_2^1, i = 1,2,\dots,A; \tag{5}$$

$$b = 1,2,\dots,B$$

Subspaces creating the particular domains must be conjuctive.

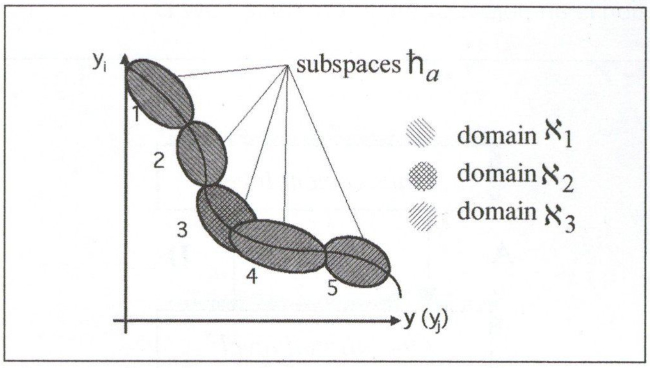


Fig. 4 Example of the subspaces and domains of the extended process variables

The image of the monitored process state is defined by fuzzy partition of the extended system of the process variables with one following method:

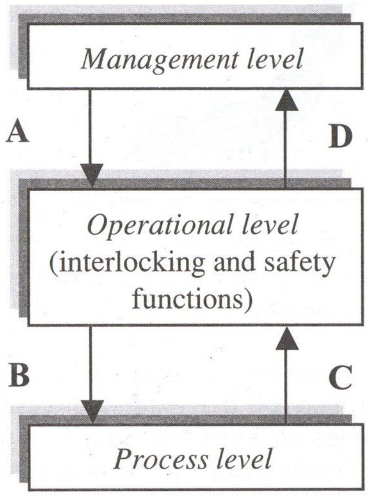
1. one fuzzy state-image T_b is allocated to every domain $\aleph_b$, $b=1, 2, \dots, B$; $B \leq A$ i.e. T_b:$\aleph_b$, $b=1, 2, \dots, B$. Example: T_1:$\aleph_1 \equiv h_1 \cup h_2$; T_3:$\aleph_3 \equiv h_4 \cup h_5$ in Fig. 4,
2. if the domain is created with exactly one subspace, then to every subspace h_a, $a=1, 2, \dots, A$, one state-images will be assigned T_a, i.e. T_a:h_a, $a=1, 2, \dots, A$. Example: T_2:$\aleph_2 \equiv h_3$ in Fig. 4,
3. combination of the methods ad 1, and ad 2,.

Let state-images T_i, T_j, where $i, j=1, 2, \dots, e$ are set to domains $\aleph_{b_1}$, $\aleph_{b_2}$, where $b_1, b_2=1, 2, \dots, B$ which are creating an adjacent segment of the domain chain. If $\aleph_{b_1} \subset \aleph_{b_2}$, or $\aleph_{b_2} \subset \aleph_{b_1}$, for example $\aleph_2$, $\aleph_3$ in Fig. 4, then these state-images are non-crisp. If the domains meet each other in one point, then state-images are crisp (Fig. 4). To ensure for control system to obtain credible information, there is a necessity to decide which hypotheses is true in selected time t. Some methods for this hypotheses evaluation are presented in [2,3,4]. Criteria for hypotheses evaluation are based on static and dynamic analysis of the measured physical variables. Their evaluation could not be either binary, nor unique. This evaluation depends not only on evaluation of absolute values and gradients of state variables but also on sequence features of the safety-related critical processes. Multicriterial fuzzy decision making is considered as a suitable method [5].

Consequences for the critical process controlling

For every actual level of decentralization, control system of the safety-related critical processes has a hierarchical structure presented in Fig. 5. Information **A** creates a global control function and conditional commands. There are decision which are realized after the appropriate safety conditions are fulfilled. A result of the realization mentioned above is an information **B** consists of elementary control function and verifiable commands. State and diagnostic information about the controlled process determinates information flow **C**.

Information about the conditional command execution is an object of the informative flow **D**.



In case, that the risk rate does not allow the command execution, control operational level generates the request for the decision to superior subsystem or affords alternatives for the elementary functions execution. The decision must be received only on management level because the risk rate is explicitly higher than it is allowed for the correspond command. Function analysis of the conventional control of the critical processes assumes the control algorithm decomposition to the elementary safe control function f_i^B.

For the control optimization of the system with goal-oriented behaviour it is necessary to choose tools for the description, modeling and model analysis which are enable increasing the control precision. For the safety-related critical processes these tools have to ensure multicriterial control. It could be expected that equation is changing into:

$$if\ \left[c_1(V_1), c_2(V_2),..., c_n(V_n)\right| c_{n+1}(B_{n+1}), c_{n+2}(B_{n+2}),..., c_m(B_m)\Big],\ then\ g_i^B \qquad (6)$$

where $c_j(V_j)$, j = 1,2,..., n are the technological control conditions completed with weight information about their plausibility and $c_k(B_k)$, $k = n$+1, n+2,...,m are interlocking (protective) conditions completed with weight information about their safety rate.

Conclusion

Fuzzy set theory application for the safety-related critical process controlling allows to quantify the credibility of the information accessed to the control algorithm. The method for the safety-related critical process controlling based on fuzzy decision making mentioned in this paper exploits a new approach for monitoring of the safety-related critical process attributes. The presented method was verified at the author's department on the example of the railway track circuit state evaluation. The model of the railway track circuit and its monitoring has been created in Matlab-Fuzzy Toolbox-Simulink environment.

This work has been supported by the Grant Agency of the Slovak Republic VEGA, grant No. 1/8261/01 „The Use of Artificial Intelligence for Critical Processes Controlling"

References

1. Molnárová, M., Adaptive control of safety-related critical processes, PhD. Thesis, EF-KIZS, University of Žilina, Žilina, Slovakia, 1999
2. Hong, D.H., Choi, Ch.H., „Multicriteria fuzzy decision-making problems based on vague set theory", Fuzzy Sets and Systems 114, 2000, pp. 103–113
3. Bhattacharyya, M., Fuzzy Markovian Decision Process, Fuzzy Sets and Systems 99, 1998, pp. 273–282
4. Molnárová, M., Spalek, J., „Hypotheses Evaluation and Decision Making using Fuzzy Logic", In: 34th Spring International Conference MOSIS 2000, Rožnov p. Radhoštěm, Czech Republic, pp. 59–64
5. Molnárová, M., Spalek, J., „Fuzzy Decision Making in Critical Process Controlling", In: 35th Spring International Conference MOSIS 2001, Hradec nad Moravicí, Czech Republic, in print

Fast convergence to root signals provided by vector LUM FTC smoother

RASTISLAV LUKÁČ

Department of Electronics and Multimedia Communications, Technical University of Košice

Abstract – The aim of this paper focuses the deterministic properties of vector median-based filters. Namely, the convergence to root signals provided by a new adaptive vector approach called vector LUM FTC smoother is presented. Besides fast convergence of the proposed method, the achieved roots are characterized by a high similarity to original color image. Concerning the excellent performance of the vector LUM FTC, the proposed method is useful not only for the impulse noise suppression, however, it can be used as a preprocessing tool for the additional processing e.g. cryptography and image coding.

Introduction

In general, the tasks of the signal processing can be divided into three main points such as the removal of interference [5,10], the analysis and the extraction of some characteristics of signals, and finally, the transformation [11] of signals into more suitable form for additional processing [2,3]. In this paper, the problem of the impulse noise suppression, i.e. the removal of interference, is presented.

In many cases, visualization of vector-valued signals such as color images and satellite images can be often followed by the occurrences of image degradation caused by the impulse noise. Various occasions including failures of transmission channel, aging of recording media or man-made interference results in the color artefacts on that visual human system is more sensitive.

Sufficient tool for the impulse noise suppression was proved by the ordering of input samples spanned by a filter window, where robust estimation is given by median value [5,8] of ordered set. To reject impulses from color images, there is necessary to consider correlation between color channels. If it is not that case, and color channels are processed separately, then there is applied a componentwise filter based on marginal ordering [7]. In general, component wise methods produce new vector samples, i.e. color artefacts, caused by composition of individual channel estimates.

Probably the most popular vector filter for the impulse noise suppression is vector median filter (VMF) [1,4,6,10]. In the sense of the ordering criteria, VMF is based on the reduced ordering scheme [7]. In some situation, VMF tends to distort small signal features and thus, VMF introduces a blurring that can be more objectionable than the original noise. Improved signal-details preservation has been achieved by incorporating of weights to account of an estimate. A filter class based on the reduced ordering and weight concept, called weighted vector median filters (WVMF) [10], includes VMF and center WVMF as special cases.

Although the performance of WVMF with optimal chosen weight vector is sufficient, another improvement can be achieved by adaptive weighted vector methods [4,6] with smoothing characteristics depended on statistical properties of the processed image region. These methods provide estimation near optimal filtering situation, where only noised samples are estimated whereas noise-free samples are passed to filter output without the change.

Besides traditional filtering purposes, where outliers or noisy samples are removed by the first iteration, the repeated filtration gives a mirror about the preservation characteristics of used filtering methods. When the filtering is repeated while outgoing image is unchanged, then the resulting image or signal is also called a root or a root signal. Importance of root signals lies in possibility of the use of some coding and cryptography methods that are easier to apply on the smoothed image than the rangy image. The acquisition of the proposed vector LUM FTC method is related to excellent fast convergence to root signals. In addition, the visual quality of root signals produced by vector LUM FTC is near to original.

Thus, the proposed method represents the optimal solution not only for impulse rejection [6], however, this method is characterized by excellent signal-details preserving characteristics, too.

Vector LUM FTC

The name of LUM smoothers [5] follows from their definition for scalar case, where a lower $x_{(k)}$ and upper

$x_{(N-k+1)}$ order statistics are compared with the middle sample x^* from input window. The amount of smoothing provided by LUM smoother is controlled by a parameter for the smoothing k, $1 \leq k \leq (N+1)/2$, where N is a window size. An output of LUM smoother is given by following expression

$$y_k = med\left\{x_{(k)},\ x^*,\ x_{(N-k+1)}\right\} \tag{1}$$

If x^* lies in a range formed by order statistics $x_{(k)}$ and $x_{(N-k+1)}$ it is not modified. If x^* lies outside this range it is replaced with a sample that lies closer to the median. The amount of smoothing done by the LUM smoother can range from an identity filter to that of the median.

The LUM smoothers are equivalent to center-weighted medians (CWM) [8], i.e. weighted median filters with the weight vector $w = \{1,1,...,1,w_\delta,1,1,...,1\}$, where central weight w_δ (for $\delta=(N+1)/2$) is assumed to be an odd positive integer that represents the weight of central sample x^*. Thus, for weight vector

$$w_i = \left\{\begin{matrix} N-2k+2 & \text{for } i=(N+1)/2 \\ 1 & \text{otherwise} \end{matrix}\right\} \tag{2}$$

the output of CWM filter is defined by

$$y_k = med\left\{w_1\Diamond x_1, w_2\Diamond x_2, ..., w_n\Diamond x_n\right\}, \tag{3}$$

i.e. as the median over a modified set of observations that include multiple processed samples, where multiple operator is characterized by

$$w_i\Diamond x_i = \underbrace{x_i, x_i, ..., x_i}_{w_i \text{ times}} \quad \text{for } i=1,2,...,N \tag{4}$$

To extend the scalar definition of LUM smoothers to vector case, it is necessary to consider the reduced ordering of vector samples and to express the vector LUM smoother through weighted vector median filters [10]. Let $w_1,w_2,...,w_N$ are nonnegative integer weights defined by (2) and $\mathbf{x}_1,\mathbf{x}_2,...,\mathbf{x}_N$ are input samples, then output of vector LUM smoother with control parameter k for smoothing is defined as follows [4,6]

$$\mathbf{y}_k = \arg\min_{\mathbf{x}_j \in W} \sum_{i=1}^{N} w_i \left\| \mathbf{x}_j - \mathbf{x}_i \right\|_L \tag{5}$$

where L characterizes used distance function, in general absolute or Euclidean. Note that filter output is forced to be one sample from input set $W=\{\mathbf{x}_1,\mathbf{x}_2,...,\mathbf{x}_N\}$. Similar to the scalar case [4], according to the choice of parameter k, the amount of smoothing done by vector LUM smoothers can range from the identity filter $(k=1)$ to the vector median filter $(k=(N+1)/2$

The problem is to tune smoothing parameter in order to achieve the balance between the noise suppression and signal details preservation. Naturally, this operation should be adaptive changed in the dependence on statistical properties of input set. Excellent vector LUM FTC (fixed threshold control) [6] is based on set of rules

$$\begin{matrix} \text{IF } \left\|\mathbf{x}^* - \mathbf{y}_k\right\|_L \geq Tol_k & \text{THEN } c_k = 1 \\ & \text{ELSE } c_k = 0 \end{matrix} \tag{6}$$

where in accordance with (2) and (5) $\mathbf{y}_k$ represents output of the vector LUM smoother with smoothing level k, Tol_k $(1 \leq k \leq (N+1)/2)$ are threshold values needs to be optimized and c_k $(1 \leq k \leq (N+1)/2)$ are decision parameters that form k_{opt} defined by

$$k_{opt} = 1 + \sum_{k=2}^{(N+1)/2} c_k \tag{7}$$

Note, that $1 \leq k_{opt} \leq (N+1)/2$. In the case of $k=1$ the output of (5) is still $\mathbf{x}^*$ and thus, Tol_1 and c_1 are constrained to be $Tol_1=0$ and $c_1=1$.

The output of the vector LUM FTC is given by

$$\mathbf{y}_{FTC} = \mathbf{y}_{k_{opt}} \tag{8}$$

Note, that for 3x3 window ($N=9$) and Euclidean distance L_2, the set of suboptimal thresholds $Tol_1, Tol_2, ..., Tol_5$ was found [6] as $\{0, 40, 60, 70, 110\}$.

Convergence to root signals

Analysis of the convergence to root signals belongs to the most important deterministic properties of nonlinear median-based filters. Since the output of vector median, weighted median filters and also the proposed vector LUM FTC filter is always a sample of the vector-valued input set, after some repeated passes through chosen filter, the processed signals will be invariant against additional passes through the same filter. This unaltered or constant signal is called root signal or root. Several problems [8] such as construction of root signals, determination of the shape of root signals and to count the rate of convergence are related to root signals.

This paper focuses the number of passes or iterations needed to achieve the root signals. In some situations [1,8], e.g. for one-dimensional signals, the rate of convergence can be analytically expressed. However, in the case of natural two-dimensional (2-D) image signals, this number depends on the distribution of edges and image details, eventually on noised regions, too.

In the case of general filtering operation $f(.)$ and vector input samples $\mathbf{x}_1,\mathbf{x}_2,...,\mathbf{x}_N$, where window position is determined by processed middle sample $\mathbf{x}_{(N+1)/2}$, repeated filtering can be expressed as follows

$$\mathbf{y}^{(n+1)} = f(\mathbf{y}_1^{(n)},\mathbf{y}_2^{(n)},\ldots,\mathbf{y}_N^{(n)}) \tag{9}$$

where n is an iteration number and N is a window size, where notation

$$\mathbf{y}_i^{(0)} = \mathbf{x}_i \quad \text{for } i = 1, 2,\ldots,N \tag{10}$$

characterizes input samples.

In the sense of definition (9), the processed signal is a root of a filter with filtering function $f(.)$ if and only if

$$\mathbf{y}_{(N+1)/2}^{(n)} = f(\mathbf{y}_1^{(n)},\mathbf{y}_2^{(n)},\ldots,\mathbf{y}_N^{(n)}) \tag{11}$$

is valid for input set determined by a filter window in all possible time positions, i.e. for a whole image. In other words, there exists n, when the input signal is identical with the output signal. Then n characterizes a number of iterations needed to obtain the root signal.

Experimental results

As the test image was used well-known color image Lena (Figure 1a). The noise corruption was simulated by impulse noise (Figure 1b) that is defined by

$$\mathbf{x}_{i,j} = \begin{cases} \upsilon & \text{with probability } p \\ \mathrm{o}_{i,j} & \text{with probability } 1-p \end{cases} \tag{12}$$

where i,j characterize samples position, $\mathbf{o}_{i,j}$ is the sample from original image, $\mathbf{x}_{i,j}$ represents sample from noised image and $\upsilon=(\upsilon_R,\upsilon_G,\upsilon_B)$ is noise vector of intensity random values. Note that single components of υ were generated independently.

Experimental results were evaluated through a number of iterations (NI) needed to achieve a root signals, color difference (CD) [9], and two measures computed over the mean of color channels, namely mean absolute error (MAE) and mean square error (MSE). In the case of CD, there was established the threshold value around 2.9 that characterizes the senselessness of human eyes to the color distortion.

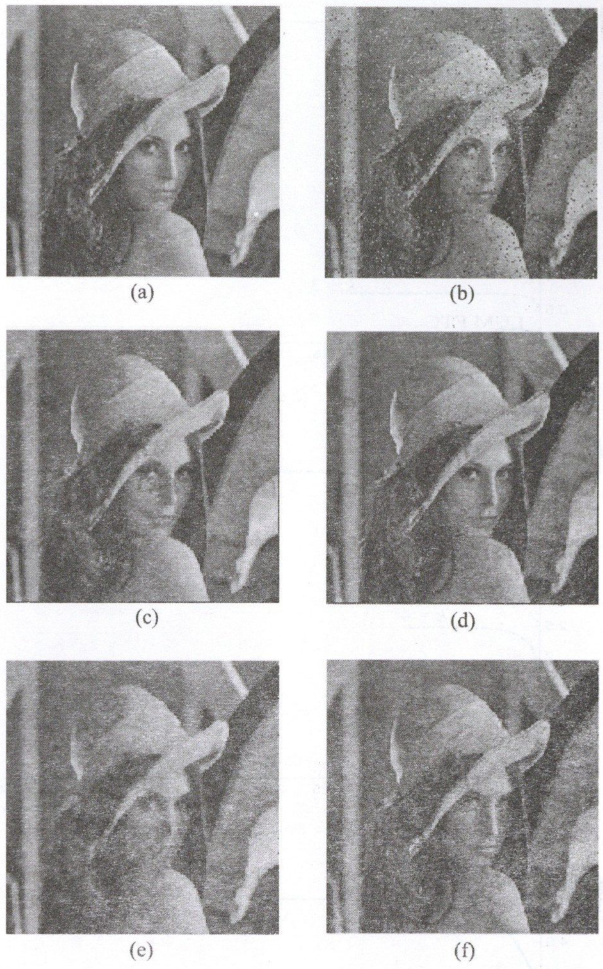


Figure 1 (a) Original image (b) 10% impulse noise (c) Output of VMF (d) Output of vector LUM FTC (e) Root of VMF (f) Root of vector LUM FTC

Obtained results are summarized in the Table 1, Figure 1 and Figure 2. The proposed vector LUM FTC (Figure 1d) achieves excellent balance between the signal-details preservation and the noise suppression. In addition, the quality of its root signal (Figure 1f) is excellent too, and both results are characterized by CD that is comparable with threshold of human eyes senselessness. The blurred results provided by vector median are shown in Figure 1c and Figure 1e. Further results are illustrat-

Image	original				p = 5				p = 10			
Method	NI	MAE	MSE	CD	NI	MAE	MSE	CD	NI	MAE	MSE	CD
Identity	–	–	–	–	–	3.762	427.3	17.406	–	7.312	832.0	32.717
Vector LUM (k=3)	23	0.755	10.0	3.028	13	1.117	22.1	4.465	11	1.517	37.4	6.059
Vector LUM (k=4)	17	2.255	33.5	9.461	16	2.479	38.5	10.321	19	2.696	43.5	11.174
Vector median	59	4.860	97.3	19.779	58	5.062	102.3	20.335	42	5.221	105.5	20.750
Vector LUM FTC	6	0.201	6.6	0.485	6	0.489	11.9	1.675	7	0.794	18.2	2.820

Table 1 Quality of root signals (L_2 norm)

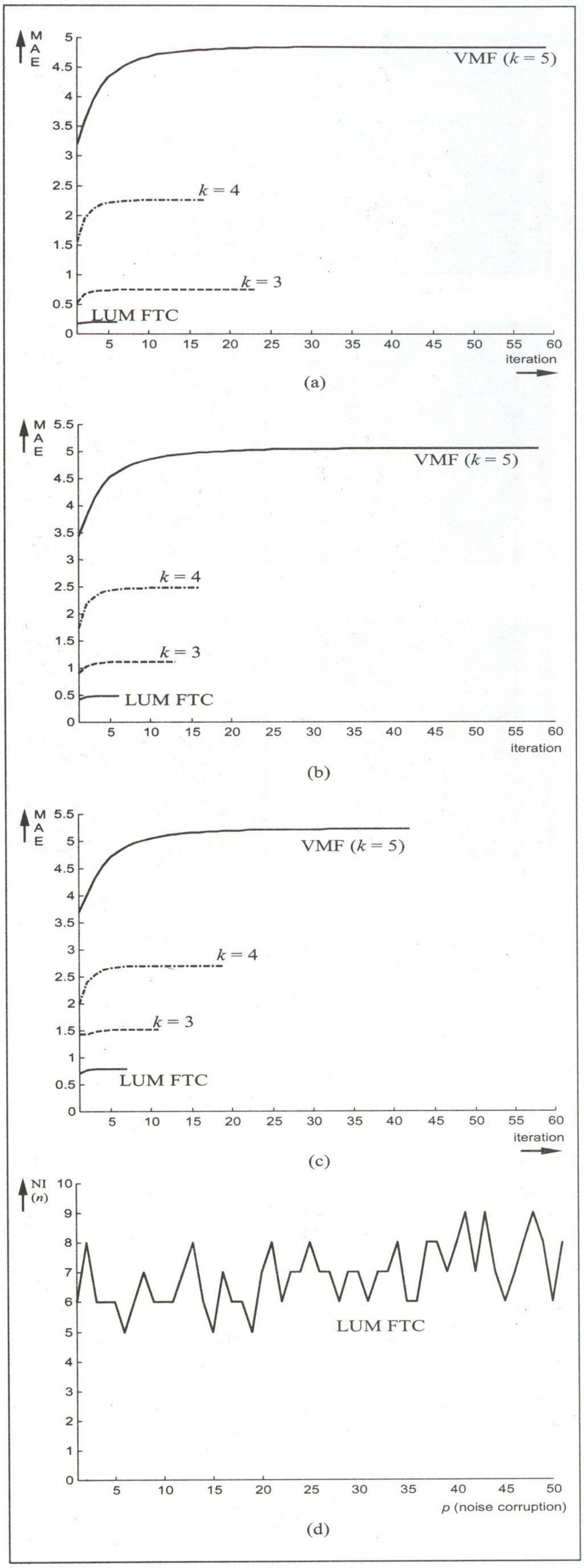


Figure 2 (a-c) Dependence of MAE on NI (a) Original image (b) 5% impulse noise (c) 10% impulse noise (d) Vector LUM FTC: Dependence of a number of iterations on a degree of noise corruption

ed in Figure 2, where the dependence of methods on a degree of the noise corruption and the behavior of MAE depended on a number of iterations is shown.

Conclusion

In this paper, the fast convergence to root signals provided by excellent vector LUM FTC method was presented. The proposed method represents sufficient toll for impulse noise suppression in color images, where signal-details preservation is required, simultaneously. Important property of the proposed method lies in a sample estimate that is forced to be a sample from the input set of vector-valued samples. It will be interesting to observe, how above properties, filter performance and excellent quality of achieved root signals can influence the additional processing.

References

1. J. Astola, P. Haavisto and Y. Neuvo, "Vector Median Filters," Proceedings of the IEEE, Vol. 78, No. 4, pp. 678-689, April 1990.
2. M. Grgic, M. Ghanbari and S. Grgic, "Texture-based Image Retrieval in MPEG-7 Multimedia System," Proceedings of the IEEE Region 8 EUROCON'2001 Conference – International Conference on Trends in Communications (Volume 2/2), Bratislava, 2001, Slovakia, pp. 365-368
3. M. Grgic, S. Grgic and M. Ghanbari, "A New Approach for Retrieval of Natural Images," Journal of Electrical Engineering, Vol.52, No.5-6, 2001, pp.117-124
4. R. Lukác, "Vector LUM Smoothers as Impulse Detector for Color Images," Proceedings of European Conference on Circuit Theory and Design ECCTD '01 in Espoo, Finland, August 28-31, 2001, pp.III-137 – III-140.
5. R. Lukác and S. Marchevsk˘, "LUM Smoother with Smooth Control for Noisy Image Sequences," EURASIP Journal on Applied Signal Processing, Vol.2001, No.2, 2001, pp.110-120.
6. R. Lukác and S. Marchevsk˘, "Adaptive Vector LUM Smoother," Proceedings of the 2001 IEEE International Conference on Image Processing ICIP 2001 in Thessaloniki, Greece, October 7-10, 2001, Vol. 1, pp.878-881.
7. I. Pitas and P. Tsakalides, "Multivariate Ordering in Color Image Filtering," IEEE Transactions on Circuits and Systems for Video Technology, Vol. 1, No. 3, pp. 247-259, September 1991.
8. I. Pitas and A.N. Venetsanopoulos, "Order Statistics in Digital Image Processing," Proceedings of the IEEE, Vol.80, No.12, December 1992, pp.1892-1919.

9. G. Sharma, "Digital Color Imaging," IEEE Transactions on Image Processing, Vol. 6, No. 7, pp. 901-932, July 1997.
10. T. Viero, K. Ostaimo and Y. Neuvo, "Three-dimensional Median Related Filters for Color Image Sequence Filtering," IEEE Transaction on Circuits and Systems for Video Technology, Vol. 4, No. 2, pp. 129-142, April 1994.
11. J. Turan, "Fast Translation Invariant Transforms and their Applications," Elfa, Košice 1999.

Rastislav Lukáč

Rastislav Lukác (Ing, Ph.D.) received the M.Sc. (Ing.) degree with distinction at the Technical University of Košice, Slovak Republic, at the Department of Electronics and Multimedia Communications in 1998. In 2001 he finished PhD. study. Currently, he is an assistant professor at the Department of Electronics and Multimedia Communications at the Technical University of Košice. His research interest includes image filtering, impulse detection, neural networks and permutations.

News

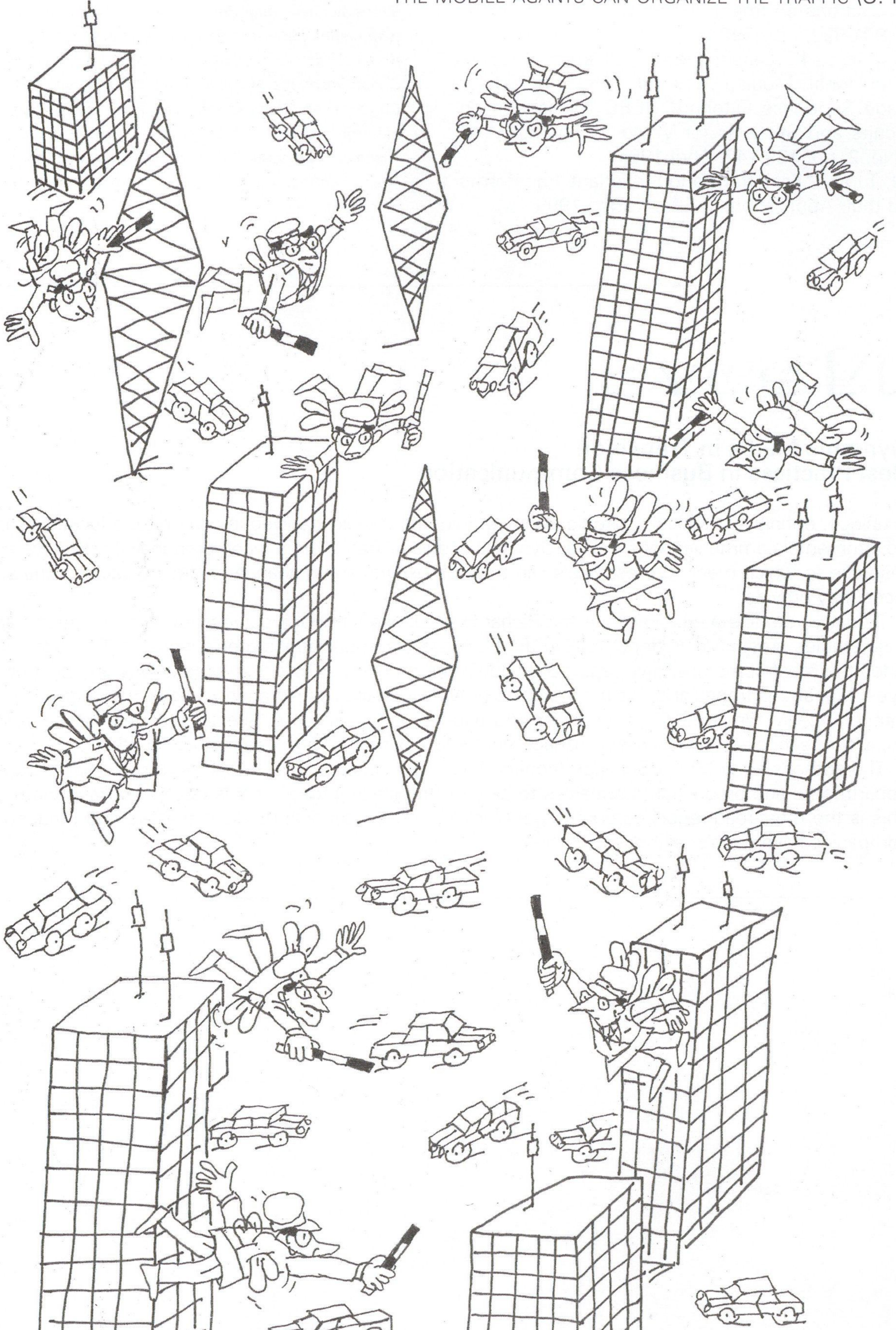
Dynamic Media in Transition
Best Practices in Business Communication

A unique, definitive practical strategic planning guide for people involved in corporate, educational and governmental communications media. Dynamic Media in Transition is a comprehensive reference and resource to which media professionals can turn for insights and guidance on adding value to the services they provide.

Industry veterans Austin Faccone and Richard Van Deusen, through surveys, extensive research and case studies present an in-depth look at the business communications media industry. This book provides the most comprehensive report ever published on budgets, staffing, productivity and best practices. It analyzes trends and, for the first time provides detailed information on how media, from print, through 16MM film to DVD is produced and used and at what cost. Special sections deal with the impact of technology, media asset management and organizational structures, amog other topics.

The author's New Media Services models define the critical success factors required for in-house departments and production companies to stay on the leading edge of this rapidly evolving industry. This is the must-read report corporate, government and educational media managers and production companies have been seeking for a long time.

THE MOBILE AGANTS CAN ORGANIZE THE TRAFFIC (S. IMRE)



Hierarchy of Rings – An Alternative Reliable Topology for IP Micro Mobility Networks

SÁNDOR IMRE, MÁTÉ SZALAY

Department of Telecommunications Budapest University of Technology and Economics

Mobile IP is the standard Internet mobility protocol. It is appropriate for global large-scale mobility but it proves to be slow in cellular mobility environment. Therefore new micro mobility protocols are required. In order to solve the routing problems easily most of the micro mobility protocols use tree based network topology. However, a serious problem of this kind of topology is its weakness in reliability. In this paper a special network topology called „hierarchy of rings" is explained. This network topology is especially designed to suit micro mobility requirements. It provides better reliability than the widely used tree topology networks, without having significant degradations in the routing capabilities.

Introduction

The 'infocom' network of the convergence, which is governing the future, will probably be based on IP. As the circumstances and requirements were different at the time of the design of IPv4, the new version of the protocol, IPv6 will have several improvements and additions. This IP based network will have to be able to handle voice traffic that requires small delay and data traffic that requires high throughput. One of the requirements that are hard and difficult to fulfill using IPv4 is the support of mobility. However, Mobile IP is an integral part of IPv6.

This 'infocom' network consists of an IP backbone and access networks. These access networks are also based on IP. The terms 'IP backbone' and 'Internet' are used interchangeably throughout this text.

Because Mobile IP [4] requires a lot of communication between the mobile node (MN) and its home agent (HA), it provides a large scale (global), but slow mobility. Below this Mobile IP mobility a small scale but fast mobility protocol is necessary. This small-scale mobility is often called micro mobility, referring to Mobile IP as macro mobility.

Micro mobility provides mobility within a well-defined area, for example an access network. The Mobile IP home agent is only notified when the mobile node leaves or enters the access network, but not at intra domain handovers. Intra-domain handovers are handled within the network, thus are very fast and do not generate any traffic on the backbone.

The IETF workgroup Context and Micro-mobility Routing „Seamoby" [8] was formed at the end of 2000. Although this is a new research field there are already several recommendations for micro mobility protocols, for example Cellular IP [5] or HAWAII [6].

In this paper a network topology called „Hierarchy of Rings" is explained in details. An overview of the micro mobility protocol that can be used over this topology is given. We are concentrating on reliability questions of micro mobility networks, but routing, handover and paging are also considered.

This paper is organized as follows: In Section 2 we give a short survey about the classical architecture of micro mobility networks. In Section 3 possible alternative network topologies are considered such as bus, star, ring, mesh. In Section 4 the proposed reliable solution for IP micro mobility topology is defined.

This paper is mainly based on [1] and [2], most of the ides are presented there.

Classical Architecture of Micro Mobility Networks

Network Topology

IP micro mobility access networks are connected to the IP backbone via gateways. Most micro mobility protocols define one gateway, and a tree topology network with the gateway as the root. Every node has one uplink neighbor (parent towards the gateway) and may have some downlink neighbors (children towards the MN). In Fig. 1 D is a downlink neighbor of C and A is an uplink one respectively. The nodes that do not have any children are called leaves. The leaves are base stations in the micro mobility network; the nodes with children are routers.

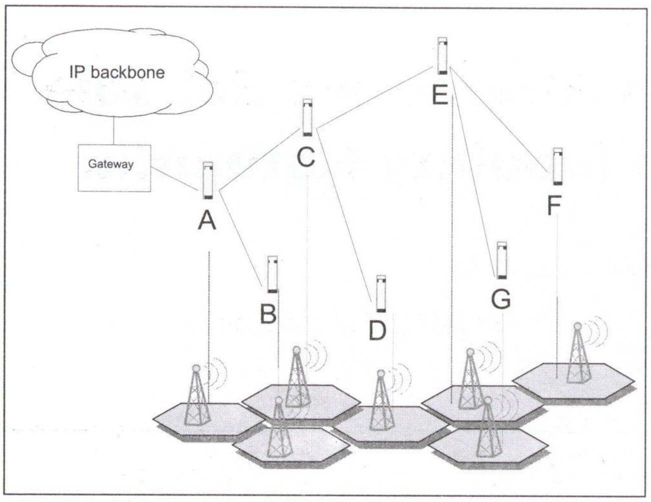


Figure 1. Classical tree-topology micro mobility network

The root node or gateway is connected to the IP backbone, and all the traffic of the mobile nodes flows through it, see Fig. 1.

Routing

Because of the wireless access, service access points (SAP) are called base stations (BS). The traffic shape of a micro mobility network is characteristic. Most of the traffic flows between a gateway and a SAP. Downlink traffic (that is sent form a gateway to a SAP) is usually much more than uplink traffic (mobile nodes (MNs) get long answers to short questions).

As MNs are wandering around within the micro mobility network, dynamic routing is needed. This makes routing an important question of micro mobility networks. The actual positions of the MNs have to be stored in a (possibly shared) database.

All the routers maintain a routing cache [7], where data is stored about the MNs that are in the subtree under the router. The routers know which child packets have to be passed to. As we go higher and higher in the tree, more and more link capacity is needed.

Uplink packets are simply passed up to the parent by every router until the gateway is reached. The routing of downlink packets is based upon the routing caches.

Reliability

Tree topology means that there is exactly one path between any two nodes. So there is exactly one path between a base station and the gateway.

This is a rather vulnerable network architecture. Consider a model, where links and nodes have two states: working/broken. If we suppose that all the traffic flows between a base station and the gateway, a link failure is equivalent to the failure of the node that is at the bottom of that link. As a result of a failure, a subtree is separated from the network.

It is even more severe, when the gateway router or the link between the gateway and the backbone breaks down. Then the whole micro mobility network is separated from the backbone, and no communication is possible between an MN in the network and another host on the Internet.

If this topology is so vulnerable, then why are almost all the micro mobility solutions based on a tree topology network? It is because the tree suits the routing requirements of the micro mobility network and signaling requirements of micro mobility protocols very well. Both uplink and downlink routing are simple so simple and relatively cheap routers can be used. And at the same time the tree is a very scalable solution. The problem that we are concentrating on is the weak reliability of the tree.

There are two basic solutions for the reliability problem. One is to use a completely different network topology; the other is to try to make the tree topology more reliable somehow. If another topology is used in the micro mobility network instead of the tree, it has to be chosen carefully. There are several aspects. The network should be less vulnerable than the tree, of course; too complex routing or too complex signaling should be avoided, and scalability is very important for micro mobility networks.

If the tree topology is kept but improved, the aspects are similar. Links and nodes have to be duplicated and physically separated for safety reasons. This new network inherits a lot of the attributes of the tree, for example it probably suits the signaling requirements, and remains scalable. But routing and signaling becomes much more complex. The micro mobility protocol and the routing have to be redesigned.

Examination of Alternative Network Topologies

In this section, we investigate various network topologies, which are suitable for micro-mobility networks. The special features of micro-mobility networks make some of the otherwise not that important aspects really crucial, and at the same time raise some new problems. The most important problems related to micro-mobility networks are:

- reliability, vulnerability,
- scalability,
- connection to other networks (Internet),
- wandering MN, complexity of routing,
- special traffic.

The tree is the „classical" micro mobility network topology. Both Cellular IP [5] and HAWAII [6] use tree network topology. Almost all requirements are met, the major weakness is vulnerability.

A bus topology network can be connected to the Internet via gateways. If multiple gateways are used, the reliability is probably satisfactory. There are no routing problems; an access protocol is used instead of routing, for example ALOHA or CSMA. The serious problem with the broadcast medium is inscalability. If it is used in a micro mobility network, the size is strongly limited.

Star is a centralized network topology. All the nodes are connected to the central node. The central node can be used as a gateway to the Internet. All intelligence can be concentrated in the central node; other nodes are very simple, thus very cheap. Routing at the central node is not very complex, and there is no routing at the other nodes. This network topology really suits the traffic shape of a micro mobility network, where most of the traffic flows between the gateway and a base station. Vulnerability is a weakness, as a central node breakdown is critical. This is one of the reasons why a double star is often used. In a double star, the central node is duplicated, and probably connected to each other. Packets then can be sent to both gateways.

Another weakness is inscalability. As the number of base stations increases, routing at the central node becomes resource time consuming.

In a ring there are exactly two paths between two nodes. If a link or node breaks down, there is still one path left, so it is much more robust than the tree. In a micro mobility ring multiple gateways should be used of course. Routing in a ring is simple. The ring does not expressly suit the traffic requirements, and inscalability is another problem. As the number of BSs increases, routing does not get more complex, but links may get overloaded.

An important ring type is the self-healing ring. In a self-healing ring only one half of the capacity is used, the other half is reserved for critical situations. It is like the MSSP (Multiplex Section Shared Protection) ring in an SDH environment. If a link breaks down, the two neighboring nodes realize the breakdown and the spared capacity of all other links is used to replace the broken link, see Fig 2. Thus, one error can be corrected below the micro mobility level, and a reliable communication network is provided for the micro mobility protocol.

To find a detailed explanation of ring topology micro mobility networks see [2].

A full mesh is nonsense of course, because it is extremely inscalable, and does not suit the traffic shape anyway. A partial mesh can be scalable and multiple gateways can be used. It is robust, if there are several paths between any two nodes. The only problem is that routing becomes difficult. The packets have to be routed correctly even when some of the links are broken. So a complex routing protocol has to be used, and all of the nodes have to function as routers, so unless a very sophisticated routing is used, it is an inefficient and expensive solution.

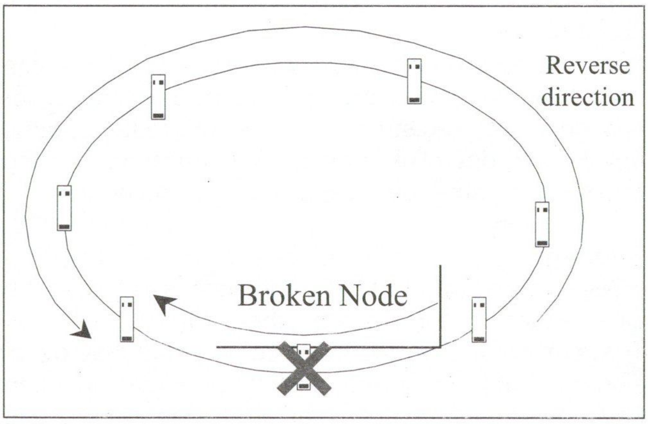


Figure 2. Self-healing ring with broken node

The Hierarchy of Rings

Topology

One method to improve the reliability of the micro mobility network by changes in the network topology was to make some changes to the tree topology; the other one was to use a completely different topology. We are trying to combine these two methods: improving the reliability of the tree topology by using a completely different network topology.

In a tree topology micro-mobility network every node has a parent node (except for the root), and every node may have some child nodes under it. A hierarchy of rings is similar to this topology. It is a tree with rings instead of the nodes. Every ring has a parent ring (except for the root ring), and every ring may have some child rings under it. In our network there is exactly one root ring, and all the rings are self-healing rings like described in Subsection 3.4.

By using this topology the advantages of the tree and the ring topology can be combined. We get a more reliable network topology than the tree, but the topology is similar to a tree, so a lot of ideas (i.e. routing algorithms, handover mechanisms) can be reused.

All the rings are self-healing rings, but to build a robust network that can handle failure of the interconnection links that connect the rings of the access network, every ring should have multiple connections to its parent ring.

Node Types

In a hierarchy of rings topology micro mobility network there are the following node types:

- gateway + router: The router routes the packets between the two neighbouring nodes in the ring and the gateway. The gateway sends packets out to the IP backbone and receives packets from there. There are probably about two or three nodes of this type in the access network. Our hierarchical network has gateways only in the root ring.
- BS + router (SAP): The router routes packets between the two neighbours and the BS. The BS sends packets to the MNs and receives packets from them. This is probably the most common node.
- Interconnection node: these nodes connect the parent ring with a child. There can be two functions separated in an interconnection node. It acts as a base-station-like router in the parent network, and acts as

a gateway-like-router in the child network. These two functions can even be separated physically.
- router + special function: There can be nodes that neither function as gateways nor as BSs, but have some other function such as packet authentication or traffic analysis.
- combined: We can have almost any combination of the above nodes.

Ring Types

In our micro mobility network a ring has either BS routers or child rings, but not both. Actually both of them can be allowed, but this restriction makes the network much more structured. So there are two types of rings: access rings (with BSs but no children) and transport rings (with children but no BSs).

Access rings are actually ring topology micro mobility networks with enhanced database gateways like described in [2], but with a bit more functionality. The interconnection nodes that connect the access ring to its parent act like the gateways in a simple ring structure. They have information about all the MNs connected to this access ring. Fig. 5 shows a micro mobility network with hierarchy of rings topology. This network has three access rings, two transport rings and the root ring has two gateways.

All the applied rings are self-healing rings, so one error in a ring is corrected below the IP level. Every ring has a parent ring (except for the root ring), and every ring may have some child rings under it. To build a robust network that can handle failure of the links that connect the networks, every ring should have multiple connections to its parent ring, and the root ring should have multiple gateways. The multiple connections have to be also physically independent. Rings that are in the leaves of the tree will be called access rings, other rings are the transport rings.

Reliability

From reliability point of view a graph model is used, where links are the edges, and hosts are the vertices. Links have two states: working/broken, they are stochastic variables, independent (at least until the occurrence of the first error), and the error probability is fairly low. The performance of a system that tolerates one error is much better than the performance of a system that is not able to tolerate any errors.

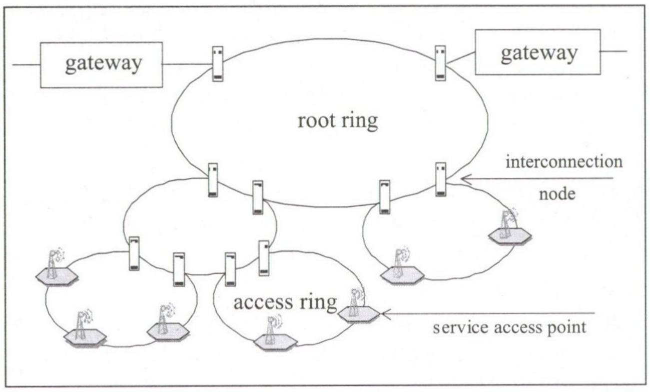


Figure 3. Hierarchy of rings network topology

In our two-state model a node breakdown is equivalent to a simultaneous breakdown of all the links of that node. Our proposed network topology can tolerate one node or link error. As a node breakdown is more „severe" than a link breakdown, it is enough to examine node breakdowns.

If a SAP breaks down in an access ring, the ring heals itself, and the micro mobility protocol is not even affected. Some connections may be dropped, but the network continues to function normally.

The ring from the interconnection node viewpoint towards the gateway is called the uplink ring, the ring towards the MN is the downlink ring. In case of an interconnection node breakdown, both the uplink and the downlink ring heal themselves. The topology remains the same, only the number of interconnections is decreased by one. As there are more than one interconnections between any to neighbor rings, the two rings are still connected.

If a gateway breaks down, the number of gateways is decremented by one, but as we have more than one gateways, there is still at least one left.

Our hierarchy of rings topology can surely tolerate one node or link error, and if the error positions are not very unluckily distributed (e.g. all the gateways fail), it can probably tolerate even more.

The hierarchy of rings can be considered as a tree, where the functions in a node are separated. For example interconnection nodes maintain the databases of the MN positions, gateways connect the network to the Internet, but do not do any routing.

Topology changes caused by failures should be handled by the micro mobility protocol. Uplink packets should be passed up to the parent ring by the first interconnection node they have reached. In case of an interconnection node failure, another interconnection node will pass the packets upwards. Downlink packets should be passed down to the child ring by the first adequate interconnection node. A route update messages sets up the database entries while traveling up to the root ring from a BS. It should go around all the rings on its paths so that all the downlink interconnection nodes will have information about the MN.

As topology modification is not too radical, we can use tree topology based protocols with minor changes. MN registration, handover, route update, uplink and downlink traffic, authentication, paging remains the same, but over a safer, enhanced tree.

Routing

MNs send packets to a BS of an access ring over the air interface. The BS passes them to the BS router. The router launches them on the ring, and they travel along the ring until they reach an interconnection node. As the interconnection node identifies these packet as uplink packets, it passes them „up", thus launches them on the parent ring instead of forwarding them. Packets are passed up ring by ring to the root ring by the interconnection nodes. From the root ring the first gateway sends them out to the IP backbone.

When a packet arrives from the Internet, a gateway router launches it on the root ring. As all the interconnection nodes know which MNs are connected under them, the first interconnection node that has the recipient address in its database launches the packet on the child ring instead of passing it on. The packet travels down from transport ring to transport ring until it reaches the proper access ring, where the appropriate BS passes it to the MN.

It is easy to route packets correctly if all the interconnection nodes have the information about the MNs under them. It will be elaborated how these databases can be maintained.

Registration

Now let us present what happens when a MN registers to the micro mobility network and how the databases should be built up. The micro mobility registration message travels from the access ring where the MN registers, up to the root ring and all the databases are set up. The registration message travels around the whole access ring, the whole transport rings, and the whole root ring, so all the interconnection nodes and gateways can set up their databases correctly. Registration messages can be passed up by all the interconnection nodes or just the first one it reaches. If they are passed up by all of them, multiple registration messages have to be handled in the parent ring. If only the first interconnection node passes them up, then the message has to be altered by the first interconnection node so that other interconnection nodes can know that it has already been passed up.

Handover

If the MN cannot be connected to more than one base station at a time, a Cellular IP-like [2] hard handover mechanism can be used. Here soft handover is explained in detail.

Consider the two paths: the one to the old BS and the one to the new BS. Going uplink the first ring that is part of both paths is called the crossover ring. The soft handover is similar to a registration. A control message travels up to the crossover ring. There the interconnection nodes that connect the crossover ring to its parent know that the MN is under them, they do not change the entries in their databases. A registration update message can be sent up to the root ring to prevent database entries from timing out. The interconnection nodes that connect the crossover ring to its child ring that is on the path towards the old SAP delete the database entries, so they do not route the packets down any more. A release signal may be sent down to the old BS that tears down the database entries, but they will time out anyway. During the time of the handover the MN may send packets to both BSs, and packets may arrive from both BSs. If a release signal is sent down, it can be passed to the MN, so the MN knows that it will not receive any more packets from the old BS.

The handover mechanisms of the hierarchy of rings topology networks are examined in detail in [3].

Standby Mode, Paging

MNs that are not transmitting or receiving any data may switch to „idle" state to prolong battery life. When the MN is in idle state, it does not have to notify the network about each handover, hence the network does not know its exact location. In order to locate the MN in case of an arriving packet, Paging Areas (PAs) are defined, and the MN has to notify the network only when it moves from one paging area to another. The network knows which paging area the idle state MN is staying in, but does not know its exact location.

It is obvious to define the paging areas as the access rings. When an MN switches to idle state, a message is sent around the ring, all the BS routers delete the MN from their database, and all the interconnection nodes put a paging entry in theirs.

When a packet arrives to the MN, it is routed down to the appropriate access ring, where the interconnection node sends a paging message around which makes the MN register at one of the SAPs and it switches to active state.

When the MN moves from one access ring to another in idle state, it has to notify the network. This case is very similar to a handover in active state. The MN sends an idle registration message to the new BS in the new access ring. This idle registration message travels around the new access ring. All the interconnection nodes put the paging entry in their databases, and from this point exactly the same procedure happens as in case of normal active state handover. The message travels up to the crossover router, and the path to the old access ring may be cleared explicitly or they can just left to be timed out.

For more on idle state handovers in hierarchy of rings topology networks see [3].

Conclusions

In this paper the possibilities of building a robust micro mobility network were considered. We focused on alternative network topologies. The classical micro mobility network topology use the tree topology, here some other topologies were examined as well. The presented solution is the substitution of the nodes with simple networks in a tree topology network. After that a short overview was given how the various micro mobility specific problems can be handled in a network, where ring network topology is applied at the nodes of a tree. This way the scalability and simple routing of the tree and the robustness of a ring can be combined, and the result is a safe, scalable hierarchy of rings network topology.

Acknowledgments

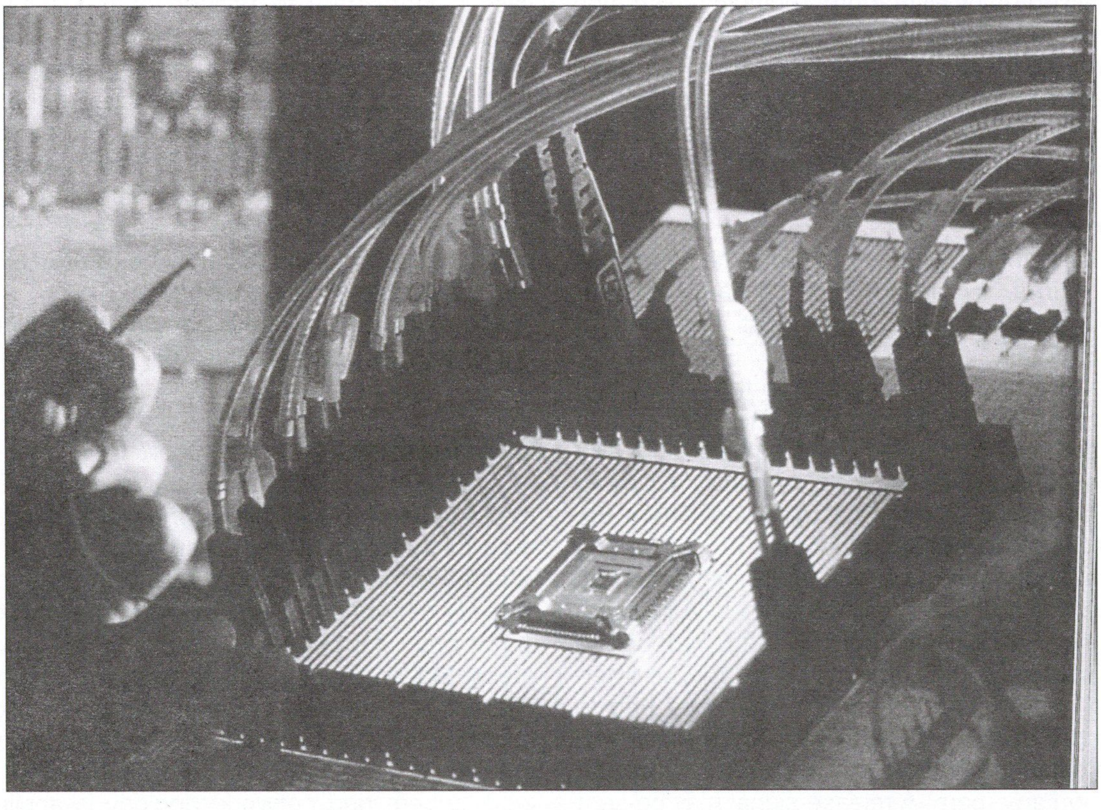
The project is supported by OTKA F032268, (Hungarian Scientific Research Found)

Abbreviations

HA	(Mobile IP) Home Agent
FA	(Mobile IP) Foreign Agent
MN	Mobile Node
IP	Internet Protocol
IETF	Internet Engineering Task Force
SAP	Service Access Point
BS	Base Station
MSSP	Multiplex Section Shared Protection
SDH	Synchronous Digital Hierarchy
PA	Paging Area

References

1. S. Imre, M. Szalay: „Reliability Considerations of IP Micro Mobility Networks", DRCN 2001, Budapest, Hungary, 7-10 October, 2001, pp.72-77.
2. S. Imre, M. Szalay: „Ring Based Reliable IP Micro Mobility Network" , ConTEL 2001, Zagreb, Croatia, 13-15 June, 2001, pp.113-120.
3. M. Szalay, S. Imre: „Handover Support in Ring Based IP Micro Mobility Networks", SoftCOM 2001, Split, Dubrovnik, Croatia, Ancona, Bari, Italy, 9-12 October, 2001.
4. C. Perkins, „IP Mobility Support", IETF RFC 2002, http://www.ietf.org/rfc/rfc2002.txt, 1996
5. A. T. Campbell, J. Gomez, C. Y. Wan, S. Kim, Z. Turanyi, A. Valko, „Cellular IP", draft-ietf-mobileip-cellularip-00.txt, IETF Internet Draft, 1999
6. R. Ramjee, T. La Porta, S. Thuel, K. Varadhan, L. Salgarelli, „IP micro-mobility support using HAWAII", draft-ietf-mobileip-hawaii-01.txt, IETF Internet Draft, 1999
7. B. Gloss, C. Hauser, „The IP Micro Mobility Approach", EUNICE 2000, September 2000, Eschende pp. 195-202.
8. IETW Working Group, Context and Micro-mobility Routing (seamoby), http://www.ietf.org/html.charters/seamoby-charter.html
9. C. Huitema:IPv6 – The New Internet Protocol, Prentice Hall, 1999.
10. C. E. Perkins: Mobile IP –Design Principles and Practices, Addison-Wesley, May 1998.
11. CA. Stephane, A. Mihailovic, A. Aghvami: "Mechanism and Hierarchical Topology for Fast Handover in Wireless IP Networks", IEEE Communications Magazine, November 2000. Pp. 112-115.



Adaptation of mobile agents in network management

GERGELY KONTRA, ANTAL MIHALYI, SZILÁRD SZABÓ, PÉTER TUBAK, SÁNDOR IMRE, RÓBERT SUGÁR

Department of Telecommunications Budapest University of Technology and Economics

Introduction: the necessity and problems of network monitoring

The use of mobile agents in some critical fields of IT holds out a great promise like management of wide area networks or cost-effective use of services. Our aim is to handle the problem of network monitoring.

Through the network evolution effective traffic control is a key issue. The previously used methods seem to be rigid under dynamic circumstances and are unable to answer correctly the problem of traffic control.

Currently, network monitoring, evaluation of traffic and decision-making of current management systems are rather centralized, and so the control-centers communicate each other by generating huge SNMP traffic on the – possibly overloaded – network. This often results in congestion, information loss, or failure of large network chunks <? Guess we could drop the last item>. Although there are suggestions and proposals how to distribute the tasks, but the problem is still open: the large amounts of data – the SNMP tables, or its parts – load the network heavily if the management systems keep their centralized nature.

Additional handicap is the lack of adaptivity in these solutions, because they hardly adapt to changing conditions. Also because rigid configuration schemes, it is hard to connect new components to the network (causing scalability problems), reconfigure the nodes, together with the unsolved proposition of software updates. When failure occurs the rigid architecture is unable or hardly able to adapt to the error.

Another drawback is that the SNMP protocol is implemented over UDP, consequently it's not guaranteed that the recipients can receive the messages. Naturally this degrades the reliability of the system. A system such as this is not fault-tolerance adequate.

To solve the previously enumerated problems, the manufacturers use product-specific objects in SNMP's MIB (Management Information Bases), or implementing proprietary management systems, we must address compatibility issues. The conventional solutions mostly use local agents, which unfortunately cannot filter the SNMP-tables efficiently, namely don't reduce traffic enough by pre-filtering. <??> These simple agents do not encorporate intelligence, they simply execute polling requests and SNMP queries where the results – often unnecessarily – traverse the network in great numbers.

Due to the mentioned problems we need a more intelligent and distributed data filtering method, which significantly cuts down the traffic control overhead. The filtering should take place locally – in the nodes, and it should not demand too much change in the existing structure. There are many experiments with mobile agents, which hold out a promise to solve the above mentioned problems. We want to take a step in this subject through a mobile agent based method. We recently developed an agent control algorithm, which seems suitable for network management tasks.

A short overview of mobile agent technologies

Before we talk about how to apply mobile agents in network monitoring, let's give a short overview about the basics of agent technologies!

A mobile agent is a software object, which

- is placed in a running environment
- has the following properties:
  - reactive: doing actions depending on its environment
  - autonomous: can influence its own functioning
  - "target oriented"
  - runs continuously in time
- may have the following properties:
  - communicative: can communicate with other objects
  - mobile: can roam from one host to another
  - „teachable": can adapt by gained knowledge

Let us show a real-life example – an internet-based search engine – to demonstrate agents can be looked at in different ways [1]! We give the conditions to the engine, which does the actual work (showing respect to a few behavior rules), and finally we get back the results. This system can be viewed as an agent system because no doubt it is autonomous: we have just told what to search and we get the results. The search engine (the agent) must take care how to achieve its objectives, while taking into consideration those "rules of the game" what its environment requires. Here we can look at the search engine as an agent system, and the searchers applied are the agents themselves.

Very similar agents come up in e-business. The main goal of these B2B (Business to Business) models is to create business connection between companies. The one, who wants to build up this connection, delegates an agent to find a prospect and somebody (it must not be the consignor) pay for this service.

What is an agent like?

Agents can be classified in three points of views:

- Mobility

  The ability of the agent to work independently of its actual location, and migrate between hosts., (it's not needed to have an owner machine) . At the lowest level the roles are static and fixed to locations, they use the client-server architecture for communication. Mobile scripts are at the next level. They can be composed on one machine and shipped to another for execution. The highest level of mobility is achieved when the agent can migrate to another host even at the middle of its work. To achieve this the agent must have the ability to save (and transfer) not only its code but also its state space.
- Degree of agency

  This property gives us information about the degree and the method of the interaction between the agent and other entities. The agent can achieve only such a place, where an environment exists that is able to receive it. An environment, which provides connection layer for agents, is called the agency. The simplest agents work asynchronous, independent of any other entities. At the next level the agents interact with data, other applications or services. The most interactive agents are those, who can communicate with other agents.
- Intelligence

  This property indicates the complexity of the agent. For a simpler agent its creator tells where and how to operate (simple configuration). If we take a look at a more complex one that makes all the difference, we cannot rely on the creator/user everything, it must be able to recognize its environment and must adapt to it. In fact there is two ways of building intelligence: knowledge-based or rule-based.

We tried to emphasize some characteristics, but decomposing the heart of the agent to primitives is nearly impossible, while an agent's action is (partly) determined by its environment, the changing of its environment, and other agents with whom it can cooperate occasionally or permanently. In practical manner we can stay that agents are simple programs, which have human attributes.

Where to apply an agent?

The greatest areas, where we can apply agents are network monitoring, information collecting and e-business (agents, brokers). Nowadays mobility is not implemented in every area where possible, despite of numerous beneficial of being an agent mobile, rather than stationary.

- Reduced network traffic

  When dealing with a bunch of data, it is wise not to transfer results of raw queries through the network, but to apply a mobile agent. This agent goes to that host, does a lot of queries there (they are local, so no need of network transmission), and just transmits the "practical result" of these queries, which can be a simple "No problem".
- Getting rid of network delay

  Very useful when repairing: the agent can take control over a computer efficient: fast and continuously. The „distance" of the controller and the controlled object mostly determines the efficiency of the controlling. If the agent goes to the machine to be repaired, then it can control it most efficient: without network traffic.
- Robust and fault-tolerant

  An agent can leave the faulty system and continue its work elsewhere if the system should went wrong totally. Agents can emerge and die whenever needed.

Security considerations

Naturally, there are some risks in using mobile agents, but the main problem is the security for sure. Running an agent on a host supposes the existence of an agency what fallows that there are two kinds of possible security holes. One could be that the agency allows running agents from an untrusted host and gives possibility to the agent for using the system's resources. If we didn't find a solution for this problem than it causes the evolution and spread of new computer viruses. On the other hand an "evil" agency can do everything what it wants with the agent's code. Although the code can be protected (for example with integrity check) the "evil" agency can modify the data carrying by the agent causing the next agency work improper.

For the sake of the security we can do the followings:

- Securing the agents' operations

  This could be an efficient protection, but in the most case it could be a disadvantage and is not fully compatible with the principles of the mobile agents namely the free resource-access to the hosts. The limitation similar to the Java language's is operable for a certain level and has the advantage for the newly joined host that it doesn't have to know anything from the outside world. This approach is likely to the following "You can do whatever you want

Adaptation of mobile agents in network management

GERGELY KONTRA, ANTAL MIHALYI, SZILÁRD SZABÓ, PÉTER TUBAK,
SÁNDOR IMRE, RÓBERT SUGÁR

Department of Telecommunications Budapest University of Technology and Economics

Introduction: the necessity and problems of network monitoring

The use of mobile agents in some critical fields of IT holds out a great promise like management of wide area networks or cost-effective use of services. Our aim is to handle the problem of network monitoring.

Through the network evolution effective traffic control is a key issue. The previously used methods seem to be rigid under dynamic circumstances and are unable to answer correctly the problem of traffic control.

Currently, network monitoring, evaluation of traffic and decision-making of current management systems are rather centralized, and so the control-centers communicate each other by generating huge SNMP traffic on the – possibly overloaded – network. This often results in congestion, information loss, or failure of large network chunks <? Guess we could drop the last item>. Although there are suggestions and proposals how to distribute the tasks, but the problem is still open: the large amounts of data – the SNMP tables, or its parts – load the network heavily if the management systems keep their centralized nature.

Additional handicap is the lack of adaptivity in these solutions, because they hardly adapt to changing conditions. Also because rigid configuration schemes, it is hard to connect new components to the network (causing scalability problems), reconfigure the nodes, together with the unsolved proposition of software updates. When failure occurs the rigid architecture is unable or hardly able to adapt to the error.

Another drawback is that the SNMP protocol is implemented over UDP, consequently it's not guaranteed that the recipients can receive the messages. Naturally this degrades the reliability of the system. A system such as this is not fault-tolerance adequate.

To solve the previously enumerated problems, the manufacturers use product-specific objects in SNMP's MIB (Management Information Bases), or implementing proprietary management systems, we must address compatibility issues. The conventional solutions mostly use local agents, which unfortunately cannot filter the SNMP-tables efficiently, namely don't reduce traffic enough by pre-filtering. <??> These simple agents do not encorporate intelligence, they simply execute polling requests and SNMP queries where the results – often unnecessarily – traverse the network in great numbers.

Due to the mentioned problems we need a more intelligent and distributed data filtering method, which significantly cuts down the traffic control overhead. The filtering should take place locally – in the nodes, and it should not demand too much change in the existing structure. There are many experiments with mobile agents, which hold out a promise to solve the above mentioned problems. We want to take a step in this subject through a mobile agent based method. We recently developed an agent control algorithm, which seems suitable for network management tasks.

A short overview of mobile agent technologies

Before we talk about how to apply mobile agents in network monitoring, let's give a short overview about the basics of agent technologies!

A mobile agent is a software object, which

- is placed in a running environment
- has the following properties:
  - reactive: doing actions depending on its environment
  - autonomous: can influence its own functioning
  - "target oriented"
  - runs continuously in time
- may have the following properties:
  - communicative: can communicate with other objects
  - mobile: can roam from one host to another
  - „teachable": can adapt by gained knowledge

Let us show a real-life example – an internet-based search engine – to demonstrate agents can be looked at in different ways [1]! We give the conditions to the engine, which does the actual work (showing respect because you can't do anything wrong". But a substantive, self-operable agent is efficient when it can reach its environment at a low level. Just think to the network management. It could be, that the agent must be able to shut down a failed host.

- **Validating the agents' origin and allowing agents just from trusted sites**
  It seems that this could be an effective protection, too, but it raises many new problems to solve. The advantage (what we are expecting) is that the agents are working at the highest efficiency by allowing all kind of operations at the agency. In this case we have to verify the agents' origin because the hosts fate trembles in the balance.
  The problem is this verifying itself. We are allowing agents just from trusted sites after checking its reliability. In this case when the agency starts we have to know all of the information about the trusted sites in this way making possible to the agency to decide about the trustiness of a newly arrived agent (for example an open-key encryption is acceptable as technical background). If we are following strictly this conception than the following problem will occur: at the startup of the host we'll fix which agents can wander. This would be a very tight restriction. The system could be flexible when an agent is allowed to authenticate another agent. This will make the number of agents adaptable and we will need less information at the startup namely one agent is enough to produce an operable system. We have now just one more problem: to find a way in which the new agency gets the authentication information of the first agent.

How to use the agent-technology in the network management

Which are the advantages of using agents? Why are these mobile agents capable to solve network problems? Which are these problems that can be solved and what are the advance of its application? In which cases is it worth using this new technology? These are the most important questions. These should we see clearly before we start realizing our ideas. Let's see the main steps of headway [4]:

- The solution is dynamic with all of its advantages. The replacement of the management algorithms is significantly easier compared to static solutions because we don't have to send out the new algorithms just to update the agent in the center. With this the new code will spread on the network and the agents will operate with this new algorithms, so the effect is "immediate".
- The technology is sparing in the meaning that the agent uses the system resources just for the time what it spends at the host and is active.
- The agent visits more hosts so it has wider information about the network and about its structure as the static one which sees just its node. This gives the opportunity to make a second level SNMP filtering to minimize the volume of the transmitted data and to make the data preparing easier.
- The solution is based on restricted individual intelligence. None of the agents has high intelligence but based on their dynamic adaptability and interaction they are able to manage an optional structured network.
- In these days the development of ad-hoc networks are especially popular research subject. The advantage of this networks are the optional structure, dynamic reconfiguration and their wide applicability. The management of these networks is easy to solve with mobile agents based on their common properties.

We would like to step forward in this area with the development of a network management and monitoring system based on mobile agents and new algorithms.

To do this, the following two key-problems must be solved:

- the size of mobile agents: because of this, significant decline of network traffic is hardly achievable, compared to the conventional methods;
- the lack of proper SNMP-table filtering algorithm.

Such an algorithm that limits the excessive growth of the agents' size could deliver the solution for the first problem. Cleverly choosing the migration algorithm, as well as decreasing the amount of data carried by the agent to the necessary minimum, can solve incidentally emerging difficulties. Many possible solutions come to word in reference to the problem of the strategy, and to the question of the necessary minimum. We are testing, comparing and examining the goodness of these different solutions by running a self-developed application under simulational circumstances.

The second question is from mathematical nature. Many different solutions have already been suggested to handle the problem, which we also would like to use when working on our task. If using these methods will not provide us satisfying results, we are possibly going to modify the filtering algorithm, to better fit to the simulation. Because of the SNMP's highly rigid structure, we plan to use a new architecture, which will – without using any tables, only on the grounds of the load indicators' local values – be able to bring a decision near to the optimum.

Our idea was to build a system that is at the same time robust, able to handle unexpected situations and not bound to only one type of network topology as far as possible.

After conciliating the contradictory interests above, we developed the following system elements and algorithm:

We consider the network as the unity of smaller territories. In the beginning the whole network is a huge domain, supervised by one mobile agent, what wanders around the nodes and collects information (traffic data) with the help of its filtering algorithm, as well as modifies the node if needed. The main point of the migration algorithm is, when it detects the overload of the agent, it gets in connection with its neighbor-agents and in a trading process it tries to hand over the task of supervising some nodes (as many as needed to eliminate the overload) to one of its neighbors.

The agent is overloaded, when the turnaround-time (the time, the agents need to pass around its domain) exceeds a pre-defined value. When the agent detects its overload sends a trade-initiating message to its neighbors. The neighbors check their own load indicators and decide on the grounds of a possibility-function whether to accept other nodes to their domain, or not. This possibility is proportional with the load of the would-be-partner.

In the beginning, or if no neighbor is available what would like to trade, this solution obviously doesn't work. Even so the agent can't remain overloaded, because it cannot complete its task. In these situations the agent can split itself into two (it also splits its domain) so the load also gets halved. If there are no neighbors who are ready to trade and the agent detects its overload, it makes a decision on the grounds of a possibility-function about its segmentation. This possibility is proportional with the difference between the measured and the optimal turnaround-time. In case of a splitting the two new agents continue their tasks in the two new half-domains. If any of the new agents detects that it's still overloaded, it can initiate a trading or a splitting process again and it happens so until a balanced state is reached.

This method can also handle changing topologies on the score of its flexibility. The nodes belonging to a certain agent's domain are stored in the agent. The nodes are also aware of their domains, as well as the time, when they were last visited. The roaming agents can detect recently added network elements by detecting that these new nodes still not have any supervising agents. After that they join them to their own domain.

The opposite situation can also occur, namely elements can step out of the network. In these situations if in an agent's domain the number of the supervised nodes falls down and there are no neighbors, who want to trade (because of their overload), the agent can initiate reunion (merge process). In this case after another probability-decision the two agents and their domains merge, and henceforward one agent supervises the common domain. When two agents join the IDs of the nodes belonging to them, as well as the collected traffic data gets merged, too.

A robust system must be prepared to accidents as well, as must be satisfactory from a fault tolerant view. Assuming the worst case if such a node goes wrong, that the supervising agent resides in, then the agent gets stuck or gets lost and the node will be unreachable from outside. In this case the domain remains unsupervised. This is only a temporary state, since the neighbors of the lost agent check every node's „last visited" attribute when visiting them. If this value exceeds a pre-defined value, one of the agents makes the node free and takes it to its own value. After it the neighbors of the newly added node are visited and so on, until all, still reachable nodes get under supervision.

Another advantage of this solution is that the algorithm can be modified or updated easily without any constraint dropouts in operation. To do so only the agents must be changed, with attention to the compatibility. This can be secured, if the newer versions are written to be compatible with the older instances, which are still in the network. Updating the agents can be done by a center, but a newer version agent instance can do that itself. To do that the agent must split into two and pick up the old agent's state and data.

The set-up of the test system

We have developed our test system in ObjectSpace Co.'s Voyager mobile agent developer platform. After developing the algorithms, we began the implementation phase, to be able to test the system under real circumstances, and if needed to modify it after evaluating the results.

The system consists of the following elements:

- Agencies:
  Their task is to provide the connection between agents and nodes. Detailed tasks:
  - provide the connection between agents and nodes
  - realize safety functions: access to the resources of the nodes must be denied for unauthorized persons or programmers
- Local data collector agents:
  These agents can be found in every node of the network, but they aren't roaming, they are static. Tasks:
  - collecting traffic data when communicating with the nodes through agencies
  - stores the ID of the node's supervisor
  - stores the time of the last visit of the node's supervisor
- Roaming agents, „supervisors":
  A type of agents, that control the domains belonging to them, in the way mentioned above, namely:
  - monitoring the domain's nodes
  - transacting trading process
  - transacting splitting
  - exploring left alone nodes

Summary

Mobile agent technology provides solution to big telecom and IT networks, as well as lowering the interventional latency and the amount of information needed to manage IT networks. The intelligent mobile agents on the one hand are capable of filtering the information, on the other hand they can intervene easily, so they increase the efficiency of the network management. In this paper we only deal with questions of network monitoring, so as the next step, we would like to find a solution to more management problems (safety, configuration, etc.) leaning on the mobile agents.

The Hungarian version of this paper was publisched in N° 6/2001 pp. 19–23 (Híradástechnika)

References

1. Dave Orchard: Intelligent Agents
2. Stallings W.: SNMP, SNMP v2, SNMPv3 and RMON 1 and 2, 3rd ed., Addison Wesley, 1999
3. Yemini Y., Goldszmit G., Yemini S.: „Network Management by Delegation", Proceedings of the 2nd International Symposium on Integrated Network Management, pp. 95-107, 1991
The Hungarian version of this paper was published in N° 6/2001 pp. 19-23 (Híradástechnika)
4. Damianos Gavalas, Dominic Greenwood, Mohammed Ghanbari, Mike O' Mahony: „Advanced Network Monitoring Applications Based on Mobile/Intelligent Agent Technology", Computer Communications Journal, special issue on „Mobile Agents for Telecommunication Applications", publication in January 2000.

AVERY MOBILE TERMINAL CAN BE A TRANSPONDER AS IT IS DESCRIBED BY PROF. S. IMRE

Protection or restoration: a generic study on the impact of line costs and switching costs on the strategic decisions

ZSOLT LAKATOS[1], TIVADAR JAKAB[2]

Budapest University of Technology and Economics, Department of Telecommunications

1: PhD. student, 2: Permanent staff member

Introduction, motivations

Protection and restoration related resilience schemes can be implemented in transport networks with different technologies to realize networks with services requiring high availability connections. Dedicated 1+1 protection switching based scheme result in high extra capacity needs, and offer fast and simple operation and fast recovery time. Due to the shared resource utilization less extra resources are needed to implement restoration, however the recovery mechanism are more complex and therefore, slower for restoration. Since numerous higher level applications are sensitive for the down time of the supporting connections, there are several proposals to speed up restoration applying for example distributed algorithms [1] or ring-like topology based solutions [2].

Both protection and restoration based resilience schemes need extra node (switching) and line (transport) resources. If the reaction speed and recovery performances of both techniques are in the acceptable range, it is the economical aspect to decide which scheme to apply protection or restoration in a given networking environment.

The aim of this paper is to propose a unified model to analyze 1+1 dedicated protection and restoration, and the analysis is focused on the impact of the rate of transport and switching costs on the optimal resilience solutions.

General Protection and Restoration Schemes

To implement a 1+1 dedicated protection scheme two physically disjoint paths are required. The transported information permanently bridged into both path at the source end, and it is the receiver end which decides on the quality of the signals received from both directions, and switches over from one path to another in case of any degradation or failure. Disjoint path requirements results in duplicated end to end capacity needs.

In case of n:m shared protection n working entities (subject of independent failures) are sharing m protection ones. The sharing of protection resources implies more complex working mechanisms and switching scheme, since in case of a failure switching should be performed at the both ends of the connection. Furthermore, communication is required between the endpoints to synchronize the switching action. The extra resource needs of n:m shared protection scheme depends on the sharing ration (n:m). In the practical case n>m the amount of required extra line capacities are less then in case of 1+1, however, the number of required switches to implement n:m is definitely higher.

Dedicated 1+1 and shared n:m protection schemes are applied to protect point to point network resources like path, multiplex, regenerator and amplifier sections. Restoration is a network level resilience technique, where nodes are equipped with appropriate flexibility to establish failure state dependent routes based on re-configurable shared spare transport capacities. Complex switches (cross-connects) realize the appropriate node flexibility supporting not only the restoration, but in the general network flexibility, as well.

Based on the overview of protection and restoration schemes, the trade-off between extra transport and extra switching capacities can be identified. However, numerous valuable publications with significant novelties on network resilience related analysis and design usually focused on line cost issue only (see e.g. [2,3,4,5,6]). Dedicated 1+1 protection with high extra transport (line) capacity needs and with a few switches, shared n:m protection can be considered as an attempt to decrease the amount of extra line capacities applying more switches (and more complex operation in point to point relations). Restoration improves this idea, applying more switches and more complex operations based on network level management further, thus the reductions in extra transport (line) capacities can be achieved.

With other words the reduction of resilience oriented extra transport (line) capacities can be achieved by applying more switches and more complex operation. Focusing on the first part of the above statement a question is rising: "Under what conditions it is worth to reduce extra line capacity paying for that in increased number of extra switching units?". Or re-formalizing the above question more directly: "What is the impact of transmission cost/switching cost rate on the economical resilience solution?".

Problem Description and Modeling approach

A proper network model is needed to study the question. The basic idea of the model is to enable the selection of restoration paths with optimal number of switched hops in order to reduce extra switching costs. To achieve this type of solutions paths bypassing the switching nodes should be modeled. Therefore, additional links are introduced into the model with specified routs. These links represent line systems between not neighboring cross-connects, and these systems bypass intermediate cross-connects without interruption.

Theoretically, the network model should have been upgraded to a full mesh with multiplied links (where the multiplicity of each link is the number of routes between the endpoints in the network) according to this approach, however, simple technical and networking constraints limit the number of additional direct links significantly. A further reduction can be achieved, taking into account, that resilience schemes are designed to protect single network failures in practice. Thus, instead of a full mesh model, the initial graph model of the network can be adopted to the problem under study adding one more edge between neighboring nodes and to extra edges between not neighboring nodes. The additional edges representing the disjoint minimal routes between the nodes, i.e. an additional edge is failed when any edge via the represented route is failed. Thus, at least one route is available in the model in case of any single failure.

Applying the above model extension, the size of the model is increased. The original network model is a G(N,E) graph, with nodes |N|=n and egdes |E|=e. The extended model includes:

- e more edges (one extra edge between neighboring nodes)
- 2(n-e) more edges (two extra edges between not neighboring nodes).
- The number of nodes remains unchanged.

Thus, the extended model G*(N, E*) consists |N|=n nodes, and |E*|=e+e+2(n-e)=2n edges.

Based on the network model the well-known integer linear programming (ILP) path based formulation [7] of stand-by network dimensioning problem is applied to elaborate case studies. (There are (1+m)e+e conditions and (1+p)e+e variables in path formulations, where m represents the number directly connected pairs, and p represents the number of path to be rerouted in case of failures. The ILP formalization is applicable since the node capacity is studied on port basis.)

Results and analysis

The results represent several cases for a 10-node small network example: from 10:1 to 1:100 transport vs. switching cost ratio.

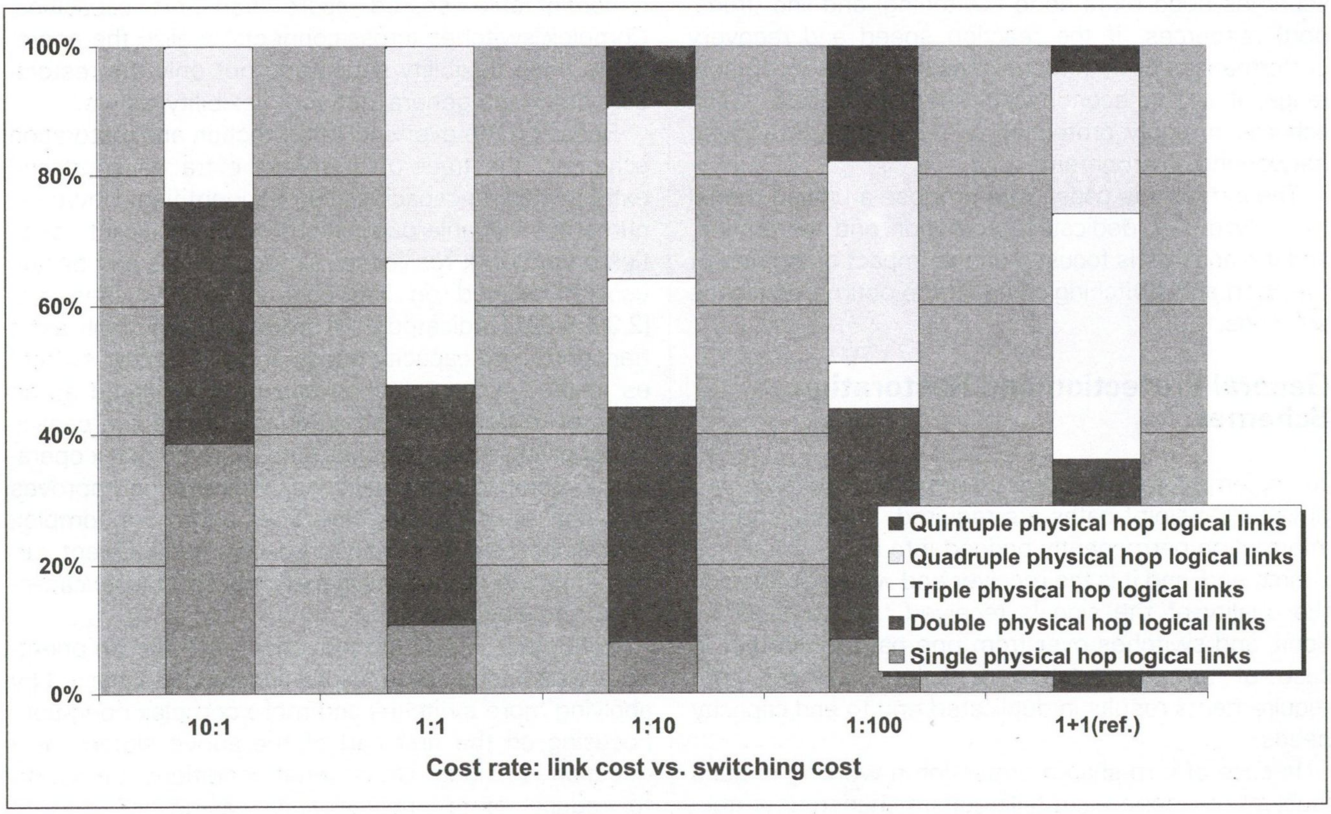


Figure 1. The relative weight of different logical link capacities in total protection/restoration link capacities

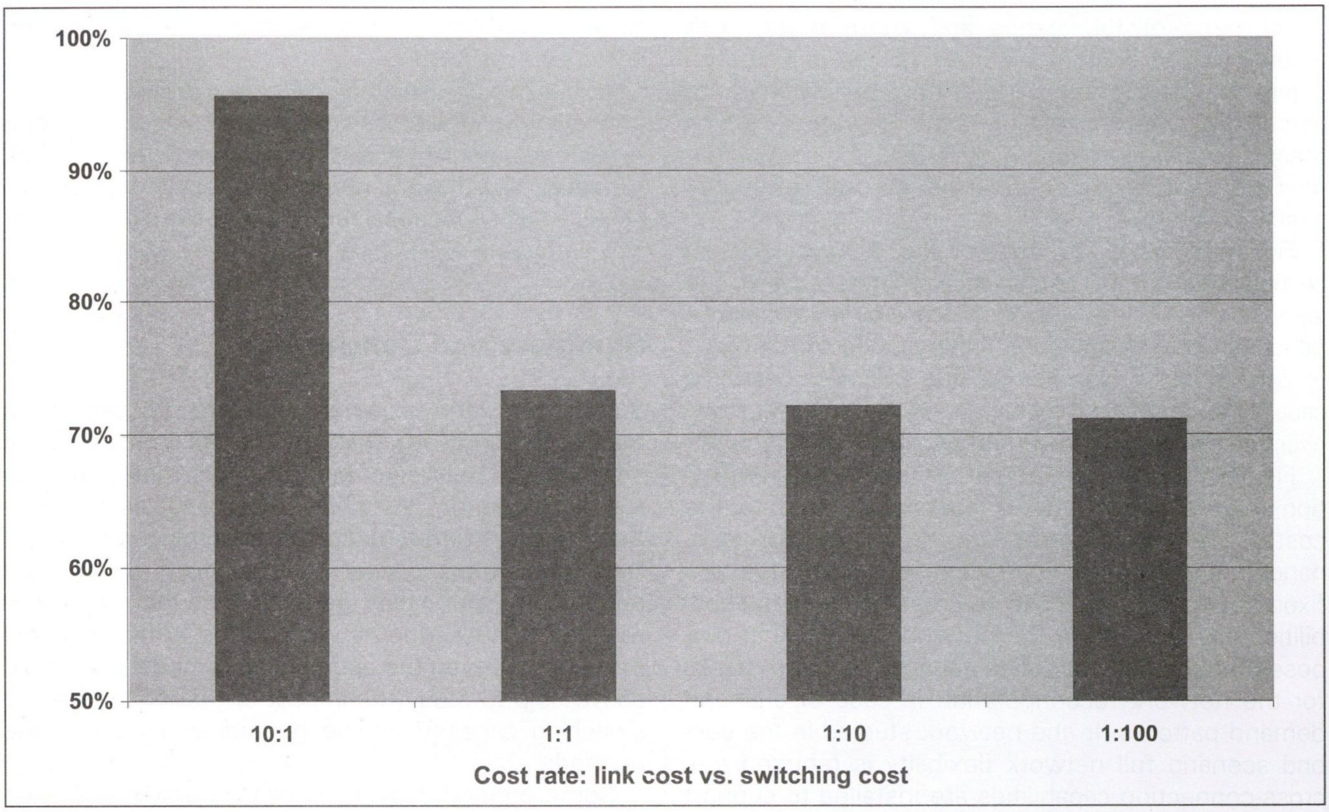


Figure 2 Path reconfiguration related switching capacity relative to termination related switching capacity (Switching capacity is represented by the number of ports in switches)

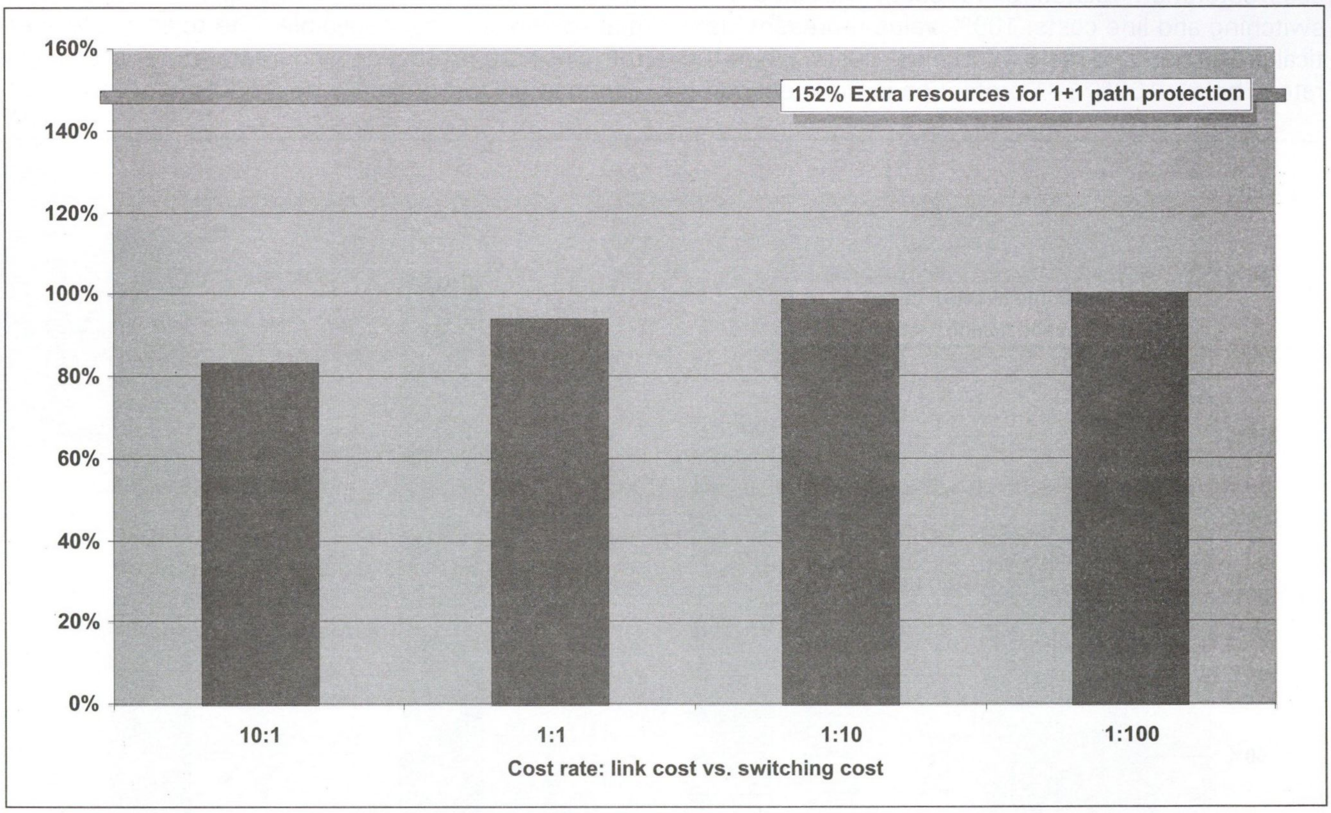


Figure 3 Resource needs in terms of channel-kilometers in different cases

Figure 1 shows the relative weight of logical links – terminate on switches- over different number of physical hops in total protection/restoration capacity. According to the presented results increasing switching cost results in increased weight of logical links over multiple physical hops, since it is less economical to install switches and decrease the extra link capacities by improving the sharing based on improved switching flexibility.

The ratio of termination and intermediate (path reconfiguration related) switches can be depicted on Figure 2. The number of intermediate switches are decreasing with increasing switching cost, which means, that the rerouting paths bypassing some intermediate switches are preferred in case of higher switching costs.

Figure 3 gives and overview on the resource needs (in terms of total number of channels) in different cases. The slow increase of the amount of stand-by resources can be identified, when longer rerouting paths are preferred to bypass expensive intermediate switches. The extra capacity for restoration is between 80% and 100%, however, the same figure for 1+1 protection is about 150%.

Figure 4 depicts the ratio of protection and restoration related extra network costs compared to the cost of the unprotected network. Two network scenarios are presented. First scenario is dedicated to a fixed network. In this case no cross-connection capabilities are required in the network for working purposes, i.e. cross-connection capabilities are required for the network reconfiguration in case of changed demand patterns. In the network studied in the second scenario full network flexibility is required, i.e. cross-connection capabilities are installed to support both working and resilience. Figure 4 shows the ratio of extra costs for resilience (1+1 related extra cost/restoration related extra cost), including both switching and line costs. 100% value represent identical protection and restoration extra costs, when the rate is below 100% 1+1 protection is more economical, however, for values higher than 100% restoration cost performs better.

As it is can be depicted on Figure 4 in case of a fixed network when the cross-connection costs present due to restoration only, 1+1 protection is more economical. However, in a flexible network, where cross-connection is a basic functional requirement the extra cost for 1+1 with general flexibility is extremely high.

Summary and Conclusions

Summarizing the experiences with the developed model is approved, that the model is capable to describe the networks with potential routes bypassing cross-connect switches, thus, enables to study the impact of different line vs. switching cost ratios. Switches in transport networks supports not only the restoration, but the general network flexibility required to adopt the network to the traffic changes, as well. However, the approach and model presented above help to study the impact of resilience oriented switching capacity on the general economy of the network.

Some general conclusion can be drawn based on the illustrative study of the small network examples. Studying different protection and restoration schemes the impact of switching cost on the optimal solutions is not negligible. The relative cost performance of protection and restoration is strongly depends on the originally desired network function-

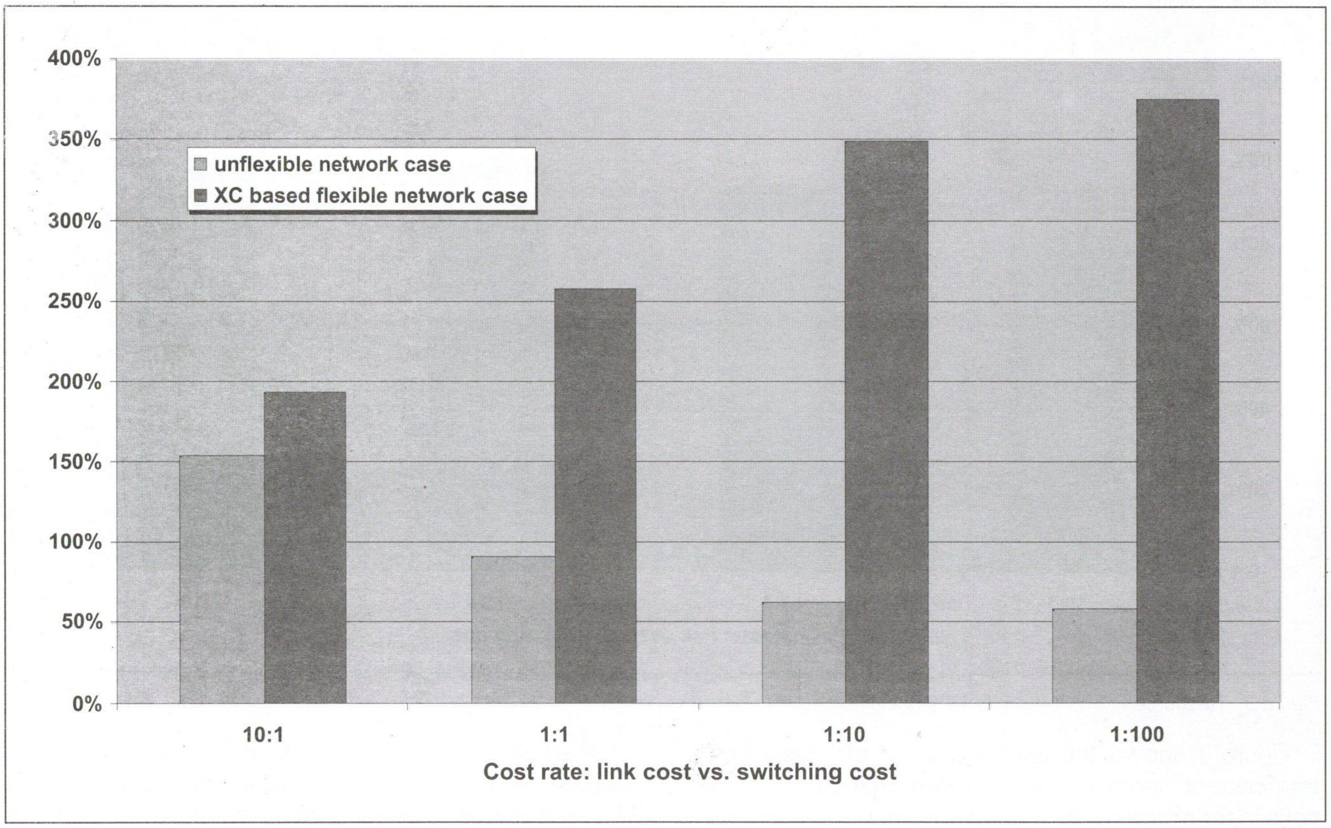
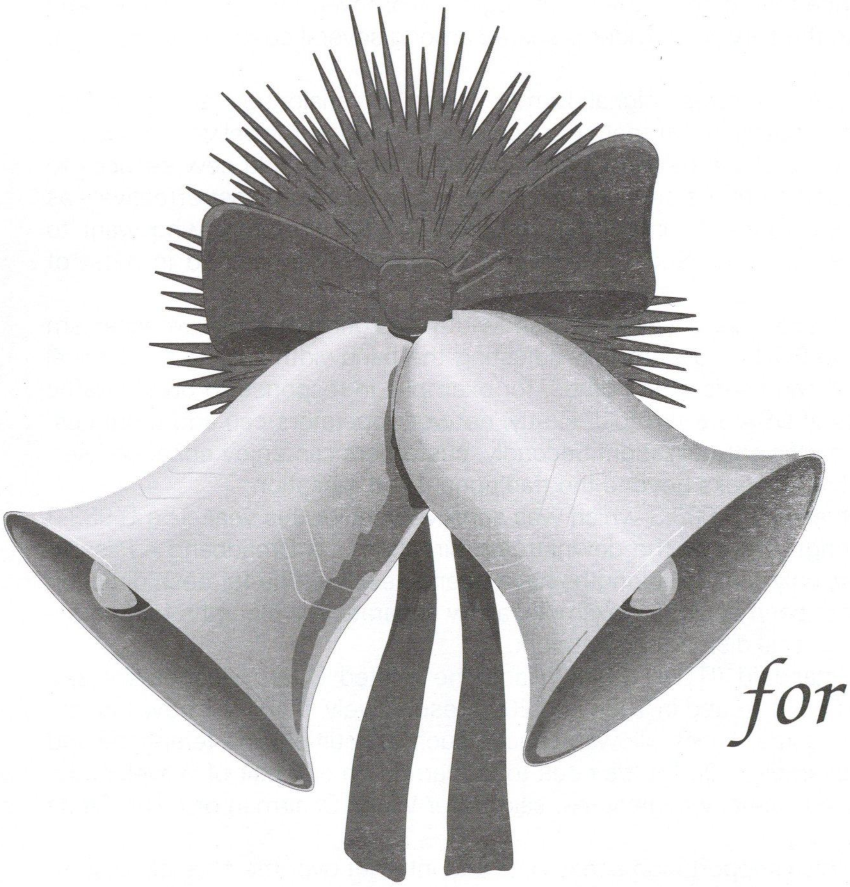


Figure 4 Ratio of protection and restoration related extra network costs compared to the cost of the unprotected network

ality. If a fixed network is required, 1+1 protection can be a simple and effective solution to achieve required network resilience. However, if general network flexibility is required and it is the very case under uncertain traffic conditions, based on the cross-connects installed work normal operation purposes restoration is definitely the economical resilience solution.

References

1. R. Iraschko et al.: A distributed real time path restoration protocol with performance close to centralized multi-commodity max flow, DRCN98 Workshop, Brugge, Belgium, 1998.
2. W.D> Grover , D Stamatelakis: Bridging the ring-mesh dichotomy with P-cycles, DRCN2000 Workshop, Munich, Germany, 2000.
3. D. Johnson: Survivability strategies for broadband networks CLOBCOM'96, London, GB, 1996
4. M. Gryseels et al..: A cost evaluation of service protection strategies in ATM on SDH transport networks, DRCN98 Workshop, Brugge, Belgium, 1998.
5. M. Gryseels P. Demeester.: A multi-layer planning approach for hybrid SDH-based ATM networks, 6th International Conference on telecommunications Systems, Nashville, TE, US, 1998
6. J. Doucette, W. Grover: Comparison of mesh protection and restoration schemes and the dependency on graph conectivity, DRCN2001 Workshop, Budapest, Hungary, 2001.
7. U. Mocci: Stand-by network optimization – Network modeling and solution techniques, COST 201 Technical Report, 1981



We wish
a merry
Christmas
and a happy
New Year
for every reader

Editorial Board

News

Bringing broadband to the home

A passive optical network (PON) is a system that brings optical fiber cabling and signals all or most of the way to the end user in residential and new small/medium business networks. Depending on where the PON terminates, the system can be described as fiber-to-the-curb (FTTC), fiber-to-the-building (FTTB), Fibre To The Cabinet (FTTCab), Fibre To The Office (FTTO) or fiber-to-the-home (FTTH).

Passive Optical Networks (PONs) utilize light of different colours (wavelengths) over strands of glass (optical fibres) to transmit large amounts of information between customers and network/service providers. The passive simply describes the fact that optical transmission has no power requirements or active electronic devices once the signal is going through the network. With PONs, signals are carried by lasers and sent to their appropriate destination by devices that act like highway interchanges, without the use of any electrical power, eliminating expensive powered equipment between the provider and the customer. PONs offer customers video applications, high-speed Internet access, multimedia and other high-bandwidth capabilities.

Although the technique of PONs has been known for around 20 years as an alternative to traditional wire pair and coaxial cable, it is only now, with the need for fast internet access, that they are looking attractive for mass deployment in, for example, new building developments. Line rates are up to 622 Mbit/s in both the upstream direction (customer to network/service provider), and the downstream (network/service provider to customer) direction – over three to four orders of magnitude (or 1,000 to 10,000 times) faster than a state-of-the-art modem which provides for network access at up to 56 kbit/s. In addition to speed, another advantage of optical technology is that it is flexibile and is expected to require less maintenance than older cable technologies. Moreover, the costs of fibre and much of the aquipment located with the service provider is shared among several customers, making it more cost-attractive.

Because PON is indpendent from bit rates, signal format (digital or analogue), and protocols (SONET/SDH, Internet Protocol, Ethernet or ATM), only the equipment needed for delivering specific services needs to be added at the ends of the network when the time comes to add new services to existing customers or to add new customers. As services can be mixed or upgraded cost-effectively as required, PONs offer the type of scability – an important consideration for operators who want to expand capacity in line with market demand. Such a degree of flexibility is unmatched in most of today's network architectures.

The draft new standard G.983.4 specifies a Dynamic Bandwidth Assignment (DBA) mechanism which improves the efficiency of the PON by dynamically adjusting the bandwidth among the Optical Network Units (ONUs) that are near end users or in homes, for example, in response to bursty traffic requirement.. The practical benefits of DBA are twofold. Firstly, network operators can add more customers to the PON due to the more efficient utilization. Secondly, customers can enjoy enhanced services, such as those requiring bandwidth peaks beyond the traditional fixed allocation.

These draft new standards complement G.983.3 which was approved earlier this year. The G.983.3 standard adds an additional wavelength band to the downstream direction of a Broadband – Passive Optical Network (B-PON). Until now, only two wavelengths have been specified, one for each direction of transmission. The new wavelength band could, for example, allow separate wavelengths for interactive and broadcast services over an optical distribution network.

Together with the basic PON standard (ITU-T G.983.1) and the related PON management and control interface standard (ITU-T G.983.2) issued in 1998 and 2000 respectively, the ITU-T now furnishes a consistent set of five PON standards, which allows services such as multiple-line telephony and high speed internet access at, for example, 100 Mbit/s rates to be carried on one pair of wavelengths and video services on one or more additional wavelengths, said Peter Wery, Chairman of ITU-T Study Group 15.

Vendors already have products which support high-speed data and internet over the fibre accessnetwork and work is now starting in the ITU-T on standards for TV multiplexing and modulation schemes for the broadcast overlay.

Application of momentary Fourier transform to burst-mode SAR processing

SANDOR ALBRECHT

Ericsson Hungary
Research and Development

A common technique in signal and image processing is to extract a portion of the signal by windowing, and then perform the DFT on the window contents. The momentary Fourier transform (MFT) applies to the particular case where the window is moved one data sample along the signal between successive transforms. In this paper we give an alternate derivation of the recursive form of the MFT using general matrix transforms. After a detailed description of burst-mode data and SIFFT properties, we describe how DFTs and IDFTs are used in the SIFFT method of Synthetic Aperture Radar (SAR) processing. We apply the MFT and inverse MFT (IMFT) to this algorithm and show what advantages they have compared to the FFT and IFFT algorithms.

Introduction

The discrete Fourier transform (DFT) is a widely used tool in signal or image processing and its efficiency is important. There are applications where it is desirable to use relatively small, successive, overlapped DFTs to obtain the spectrum coefficients. The momentary Fourier transform (MFT) computes the DFT of a discrete-time sequence for every new sample in an efficient recursive form. In this paper we give an alternate derivation of the MFT using the momentary matrix transform (MMT). Recursive and non-recursive forms of the inverse MFT are also derived, which can provide efficient frequency domain manipulation (e.g. filtering), followed by a discussion on the efficiency of the MFT and IMFT. Uses of the incremental DFT were introduced by Papoulis in 1977 [1], and by Bitmead and Anderson in 1981 [5]. A detailed derivation of the momentary Fourier transform was given by Dudás in 1986 [6]. In 1991, Lilly gives a similar derivation, using the term "moving Fourier transform", and uses the MFT for updating the model of a time-varying system [7].

A synthetic aperture radar (SAR) is a powerful sensor in remote sensing which is capable of observing geophysical parameters of the Earth's (or another planet's) surface, regardless of time of day and weather conditions [3, 10]. SAR systems are extensively used for monitoring ocean surface patterns, sea-ice cover, agricultural features and for military applications such as in the detection and tracking of moving targets. A SAR transmits radar signals from an airborne or spaceborne antenna which is perpendicular to the flight direction of the platform which is travels at a constant velocity. The back-scattered signal is collected by the antenna and stored in a raw format. Extensive signal processing is required to produce the output SAR image.

When a SAR system is operated in burst-mode, its azimuth received signal has a segmented frequency-time energy in its Doppler history. It requires that IDFTs be located at specific points in the spectral domain to perform the azimuth signal compression. First we give a detailed description of the burst-mode data properties, than we show how the short IFFT (SIFFT) algorithm has the requirement of arbitrary-length, highly-overlapped IDFTs to process burst-mode data, in which case the IMFT is shown to have computational advantages.

Theory of momentary matrix transformation

Recursive momentary matrix transformation

Let x_i be a sample of an arbitrary complex-valued sequence of one variable. The sequence will be analyzed through an N-point window, ending at the current sample i. In subsequent analyses, the window will be advanced one sample at a time. At time i, sample x_i enters the window, while x_{i-N} leaves the window. At samples i-1 and i, the windowed function can be represented by the following two column vectors:

$$\mathbf{x}_{i-1} = \begin{bmatrix} x_{i-N} \\ \cdot \\ \cdot \\ \cdot \\ x_{i-1} \end{bmatrix}, \qquad \mathbf{x}_i = \begin{bmatrix} x_{i-(N-1)} \\ \cdot \\ \cdot \\ x_{i-1} \\ x_i \end{bmatrix} \tag{1}$$

Let $\mathbf{T}$ be an $N \times N$ nonsingular matrix, which represent a linear transformation and has the inverse $\mathbf{T}^{-1}$. The sequence of index vectors is transformed by $\mathbf{T}$ at each sample:

$$\ldots,\quad \mathbf{y}_{i-1} = \mathbf{T}\mathbf{x}_{i-1},\quad \mathbf{y}_i = \mathbf{T}\mathbf{x}_i,\quad \ldots \tag{2}$$

Let $\mathbf{P}$ be the $N \times N$ elementary cyclic permutation matrix:

$$\mathrm{P} = \begin{bmatrix} 0 & 1 & . & . & 0 \\ . & 0 & 1 & . & 0 \\ . & . & 0 & 1 & . \\ . & . & . & 0 & 1 \\ 1 & 0 & . & . & 0 \end{bmatrix} \tag{3}$$

When the vector $\mathbf{x}_{i-1}$ is multiplied by $\mathbf{P}$, a one-element circular shift is performed, such that the index of each element is increased by one, and the first element becomes the last one:

$$\mathbf{P}\mathbf{x}_{i-1} = \begin{bmatrix} x_{i-(N-1)} \\ . \\ . \\ x_{i-1} \\ x_{i-N} \end{bmatrix} \tag{4}$$

Then the $\mathbf{x}_i$ vector can be expressed by the shifted $\mathbf{x}_{i-1}$ vector and with an adjustment vector $\Delta\mathbf{x}_i$ made in the last row for the difference between the samples entering and leaving the window:

$$\mathbf{x}_i = \begin{bmatrix} x_{i-(N-1)} \\ . \\ . \\ x_{i-1} \\ x_{i-N} \end{bmatrix} + \begin{bmatrix} 0 \\ . \\ . \\ 0 \\ x_i - x_{i-N} \end{bmatrix} = \mathbf{P}\,\mathbf{x}_{i-1} + \Delta\mathbf{x}_i \tag{5}$$

Substituting eqn. (5) into the transformation associated with the *ith* window in eqn. (2) and using the inverse transform $\mathbf{x}_{i-1} = \mathbf{T}^{-1}\mathbf{y}_{i-1}$, the following relationships are obtained:

$$\ldots,\quad \mathbf{y}_{i-1} = \mathbf{T}\mathbf{x}_{i-1},\quad \mathbf{y}_i = \mathbf{T}\mathbf{x}_i,\quad \ldots \tag{6}$$

Eqn. (6) expresses the recursivity of the momentary matrix transforms (MMT), since calculation of the newly transformed index vector $\mathbf{y}_i$ is obtained from the previously transformed vector $\mathbf{y}_{i-1}$ and the difference between samples entering and leaving the window.

Diagonal form of MMT

The momentary matrix transform is particularly efficient and the elements of $\mathbf{y}$ can be calculated separately only if the similarity matrix transform $\mathbf{TPT}^{-1}$ in eqn. (6) is diagonal. The $\mathbf{P}$ matrix has N distinct eigenvalues ($\lambda_0, \ldots, \lambda_{N-1}$) which are the *nth* complex unit roots, $\lambda_k = w^{-k} = e^{j2\pi k/N}$, $k = 0,1,2,\ldots N-1$. There are N linearly independent eigenvectors that correspond to each eigenvalue:

$$\lambda_0 = w^0 = 1 \Leftrightarrow \mathbf{s}_0 = \begin{bmatrix} 1 \\ 1 \\ . \\ . \\ 1 \end{bmatrix};\ \lambda_1 = w^{-1} \Leftrightarrow \mathbf{s}_1 = \begin{bmatrix} 1 \\ w^{-1} \\ w^{-2} \\ . \\ w^{-(N-1)} \end{bmatrix};\ \ldots$$

$$\lambda_k = w^{-k} \Leftrightarrow \mathbf{s}_k = \begin{bmatrix} 1 \\ w^{-k} \\ w^{-2k} \\ . \\ w^{-(N-1)k} \end{bmatrix};\ \ldots;\ \lambda_{N-1} = w^{-N-1} \Leftrightarrow$$

$$\Leftrightarrow \mathbf{s}_{N-1} = \begin{bmatrix} 1 \\ w^{-(N-1)} \\ w^{-2(N-1)} \\ . \\ w^{-(N-1)(N-1)} \end{bmatrix} \tag{7}$$

If the eigenvectors are chosen to be the columns of the inverse of the $\mathbf{T}$ matrix, then $\mathbf{TPT}^{-1}$ is a diagonal matrix, with the eigenvalues of $\mathbf{P}$ along its diagonal:

$$\mathbf{TPT}^{-1} = \mathbf{S}^{-1}\mathbf{PS} = [\mathbf{s}_0^{-1}\ \mathbf{s}_1^{-1} \ldots \mathbf{s}_{N-1}^{-1}]\ \mathbf{P}\ [\mathbf{s}_0\ \mathbf{s}_1 \ldots \mathbf{s}_{N-1}] =$$

$$= \begin{bmatrix} \lambda_0 & 0 & . & . & 0 \\ 0 & \lambda_1 & 0 & . & 0 \\ . & . & \lambda_2 & 0 & . \\ . & . & . & . & 0 \\ 0 & 0 & . & . & \lambda_{N-1} \end{bmatrix} \qquad (8)$$

where $\mathbf{S}$ is the eigenvector matrix of $\mathbf{P}$ made up of the indicated column vectors, as given in eqn (7). The diagonalizing matrix $\mathbf{S}$ is not unique. An eigenvector $\mathbf{s}_k$ can be multiplied by a constant, and will remain an eigenvector [2]. Therefore the columns of $\mathbf{S}$ can be multiplied by any nonzero constants and produce a new diagonalizing $\mathbf{S}$. There is also no preferred order of the columns of $\mathbf{S}$ [2]. The order of the eigenvectors in $\mathbf{S}$ and the eigenvalues in the diagonal matrix is automatically the same. Therefore all $\mathbf{T}$ matrixes which satisfy the above mentioned properties will diagonalize the momentary matrix transform:

$$\mathbf{y}_i = \begin{bmatrix} \lambda_k & 0 & . & . & 0 \\ 0 & \lambda_l & 0 & . & 0 \\ . & . & . & 0 & . \\ . & . & . & . & 0 \\ 0 & 0 & . & . & \lambda_m \end{bmatrix} \mathbf{y}_{i-1} + \mathbf{T}_{N-1}(x_i - x_{i-N}), \qquad (3)$$

where $k, l, m \in \{0,1,\ldots,N-1\}$ and $\mathbf{T}_{N-1}$ is the last column of the matrix $\mathbf{T}$.

Inverse of diagonalized MMT

If $\mathbf{y}_i$ is available at each sample and the columns of $\mathbf{T}$ are the eigenvectors of $\mathbf{P}$, an efficient implementation of the inverse of the MMT can be obtained. The inverse MMT (IMMT) at time *i:*

$$\mathbf{x}_i = \mathbf{T}^{-1}\mathbf{y}_i$$

$$\mathbf{x}_i = [\mathbf{s}_0\ \mathbf{s}_1 \ldots \mathbf{s}_{N-1}]\mathbf{y}_i \Leftrightarrow \begin{bmatrix} x_{i-(N-1)} \\ . \\ . \\ . \\ x_{i-1} \\ x_i \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \end{bmatrix} \begin{bmatrix} y_{i,0} \\ y_{i,1} \\ . \\ . \\ . \\ y_{i,N-1} \end{bmatrix}$$

The first row of $\mathbf{T}^{-1}$ contains only ones, so the oldest element of $\mathbf{x}_i$ can be computed using adds only:

$$x_{i-(N-1)} = \sum_{k=0}^{N-1} y_{i,k}$$

from which the elements of the input sequence *(xi-*$_{(N-1)}$*..x*$_i$*)* can be computed from the transform domain sequence $\mathbf{y}_i$ with *N-1* sample delay.

In summary, the recursive form of the MMT is general. The following Section shows that the DFT/IDFT is the only transform which has the efficient diagonal form (eqn. (8)), as a result of its column vectors being the eigenvectors in eqn. (7) in a specific order.

Momentary Fourier Transform

The matrix of the discrete Fourier transform (DFT) and the inverse discrete Fourier transform (IDFT) have the properties described in Section 2.2, thus their columns are the eigenvectors of the matrix **P.** Choosing a specific order of the eigenvectors of $\mathbf{P}$ (columns of $\mathbf{S}$):

$$\mathbf{DFT} = \mathbf{F} = \mathbf{S}^{-1} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & w & w^2 & . & . & w^{N-1} \\ 1 & w^2 & w^4 & . & . & w^{2\cdot(N-1)} \\ 1 & . & . & . & . & . \\ 1 & . & . & . & . & . \\ 1 & w^{N-1} & w^{2\cdot(N-1)} & . & . & w^{(N-1)\cdot(N-1)} \end{bmatrix}$$

$$\mathbf{IDFT} = \mathbf{F}^{-1} = \mathbf{S} = \frac{1}{N}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & w^{-1} & w^{-2} & . & . & w^{-(N-1)} \\ 1 & w^{-2} & w^{-4} & . & . & w^{-2\cdot(N-1)} \\ 1 & . & . & . & . & . \\ 1 & . & . & . & . & . \\ 1 & w^{-(N-1)} & w^{-2\cdot(N-1)} & . & . & w^{-(N-1)\cdot(N-1)} \end{bmatrix} =$$

$$\frac{1}{N}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & w^{N-1} & . & . & w^2 & w \\ 1 & w^{2(N-1)} & . & . & w^4 & w^2 \\ 1 & . & . & . & . & . \\ 1 & . & . & . & . & . \\ 1 & w^{(N-1)(N-1)} & . & . & w^{2(N-1)} & w^{N-1} \end{bmatrix}$$

Using the fact that *w* is the *Nth* complex root of unity (i.e. $w^{-k} = w^{N-k}$), it can be seen that the columns of the IDFT matrix are the same as the DFT matrix, but they are in reverse order from the second column onwards eqn. (14). Therefore if $\mathbf{T}$ performs the DFT (eqn. (15)) or the IDFT (eqn. (16)), diagonal forms of the MMT can be obtained:

$$\mathbf{y}_i = \mathbf{F}\,\mathbf{P}\,\mathbf{F}^{-1}\,\mathbf{y}_{i-1} + \mathbf{F}\,\Delta\mathbf{x}_i =$$

$$= \begin{bmatrix} 1 & 0 & . & . & 0 \\ 0 & w^{-1} & 0 & . & 0 \\ . & . & w^{-2} & 0 & . \\ . & . & . & . & 0 \\ 0 & 0 & . & . & w^{-(N-1)} \end{bmatrix} \mathbf{y}_{i-1} + \begin{bmatrix} 1 \\ w^{-1} \\ w^{-2} \\ . \\ w^{-(N-1)} \end{bmatrix} (x_i - x_{i-N})$$

$$\mathbf{x}_i = \mathbf{F}^{-1}\,\mathbf{P}\,\mathbf{F}\,\mathbf{x}_{i-1} + \mathbf{F}^{-1}\,\Delta\mathbf{y}_i =$$

$$= \begin{bmatrix} 1 & 0 & . & . & 0 \\ 0 & w^1 & 0 & . & 0 \\ . & . & w^2 & 0 & . \\ . & . & . & . & 0 \\ 0 & 0 & . & . & w^{N-1} \end{bmatrix} \mathbf{x}_{i-1} +$$

$$+ \begin{bmatrix} 1 \\ w^1 \\ w^2 \\ . \\ w^{N-1} \end{bmatrix} (y_i - y_{i\text{-}N}) =$$

$$= \begin{bmatrix} 1 & 0 & . & . & 0 \\ 0 & w^{-(N-1)} & 0 & . & 0 \\ . & . & w^{-(N-2)} & 0 & . \\ . & . & . & . & 0 \\ 0 & 0 & . & . & w^{-1} \end{bmatrix} \mathbf{x}_{i-1} +$$

$$+ \begin{bmatrix} 1 \\ w^{-(N-1)} \\ w^{-(N-2)} \\ . \\ w^{-1} \end{bmatrix} (y_i - y_{i-\mathrm{N}})$$

Equation (15) expresses the recursive equation of the momentary Fourier-transform (MFT) [6, 7, 8, 9]. The N-element vector $\mathbf{y}_\mathrm{i}$ contains the Fourier coefficients of the N-point sequence $\mathbf{x}_\mathrm{i}$ ending at sample i. Note that each spectral component $y_{i,k}$ can be calculated independently,

$$y_{i,k} = w^{-\mathrm{k}}\left(y_{i-1;k} + x_i - x_{i-N}\right)$$

which increases efficiency if only a few frequency components need to be computed, as in the zoom transform.

On the other hand, eqn. (16) is the dual of the MFT, the recursive inverse momentary Fourier-transform (IMFT), where the N-element vector $\mathbf{x}_\mathrm{i}$ contains the N-point time sequence and $\mathbf{y}_\mathrm{i}$ contains N Fourier coefficients ending at frequency bin i. Note that each sample in $\mathbf{x}_\mathrm{i}$ can also be obtained independently and the same twiddle factors, but in different order, can be used to calculate both the MFT and IMFT.

Thus it has been shown that if the DFT or the IDFT performs the momentary matrix transform of a sequence the elements of the transformed sequence can be computed recursively and independently using N complex multiplies and $N+1$ complex adds (additional computational savings are available if the input sequence is real-valued).

Non-recursive inverse MFT

The non-recursive inverse momentary Fourier transform [6] can be expressed using eqn. (12) and (14) as follows:

$$x_{i-(N-1)} = \frac{1}{N}\sum_{k=0}^{N-1} y_{i,k}$$

from which each sample of the input sequence $\mathbf{x}_\mathrm{i}$ can be computed using adds only from the two-dimensional time-dependent spectrum $\mathbf{y}_\mathrm{i}$ with N-1 sample delay. In this way the MFT- non-recursive IMFT transform pair eqn. (15) and (18) can provide an efficient frequency-domain manipulation method (e.g. filtering), especially if many of the DFT coefficients are not needed.

If the elements of $\mathbf{x}_\mathrm{i}$ are real, taking advantage of the conjugate symmetry of the spectrum, the oldest element can be computed using only the real part Re of the spectrum:

$$x_{i-(N-1)} = \frac{1}{N}\sum_{k=0}^{N-1} \mathrm{Re}\left\{y_{i,k}\right\}$$

It has been showed in [6] that if $\mathbf{x}_\mathrm{i}$ is real, the Hilbert transform $H\{\}$ of $\mathrm{x}_{\mathrm{i-(N-1)}}$ can be obtained by summing only the imaginary part of the spectrum components:

$$H\{x_{i-(N-1)}\} = \frac{1}{N}\sum_{k=0}^{N-1} \mathrm{Im}\; y_{i,k}$$

In this case the MFT – non-recursive IMFT pair can be useful for different signal processing applications where the in-phase and quadrature component of the signal is needed (i.e. communications and radar systems).

Computing Efficiency of MFT

This section examines the computing efficiency of the MFT compared to different FFT implementations. Although "computing efficiency" has many ramifications, we will restrict our attention to the number of real "signal processing" operations (multiplies and adds) required to implement the algorithms.

Consider the case where N point DFTs are used to analyze an M-point complex-valued data record. If the window is shifted by q samples between each DFT application, where $1 \le q \le N$, then $\frac{M-N}{q}+1$ DFTs are needed to spectrum analyze the record, in the case of FFT. If the MFT is applied, M MFTs are needed, because the spectrum coefficients have to be calculated in each time samples, irrespectively of the value of q.

Then, when radix-2 FFTs are used:

$$OPS_{FFT} = \left(\frac{M-N}{q} + 1 \right) \left[5N\log_2(N) \right]$$

real operations, while in the case of MFT:

$$OPS_{MFT} = M\left[8N_c + 2 \right]$$

real operations are needed to analyze the whole record. In the equation above, N_c is the number of computed specturm coefficients, thus $N_c = N$ if all are calculated. The MFT becomes efficient relative to the FFT when the shift q is small. From eqn. (21) and eqn. (22), the number of shift between DFTs when the MFT is more efficient than the radix-2 FFT can be expressed:

$$q_{MFT} < \frac{(M-N)\left[5N\log_2(N) \right]}{M(8N_c\text{-}1) - 5N\log_2(N)}$$

As we can see from eqn. (23), q_{MFT} is function of the length of the data record M, the size of the window N and the calculated MFT spectrum coefficients N_c. In Figure 1, the shift between DFTs when the MFT is more efficient is shown as a function of the window length, with two values of N_c.

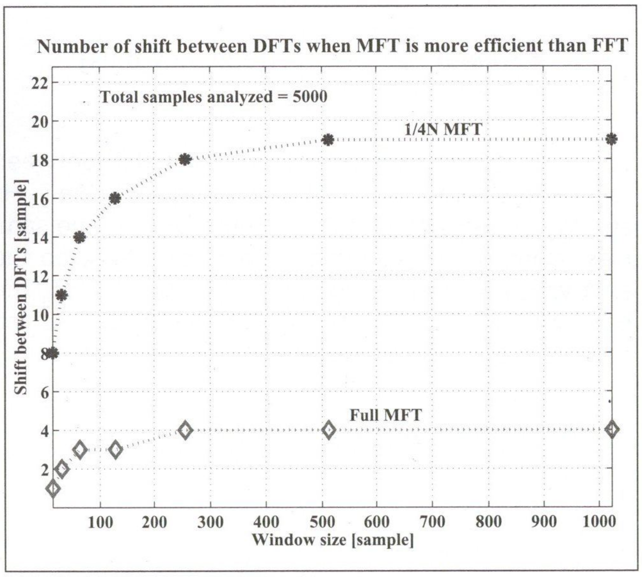


Figure 1 Shift between DFTs when the MFT is more efficient

The full MFT is more efficient compared to the radix-2 FFT, if the shift between DFTs is very small ($q_{MFT} \leq 5$), while for the reduced MFT ($N_c = N/4$), the MFT is more efficient even for larger values of shift. Note, if the data record is longer, the values of q_{MFT} are larger for all window sizes. The computational load for $q_{MFT} = 1$ is illustrated in Figure 2.

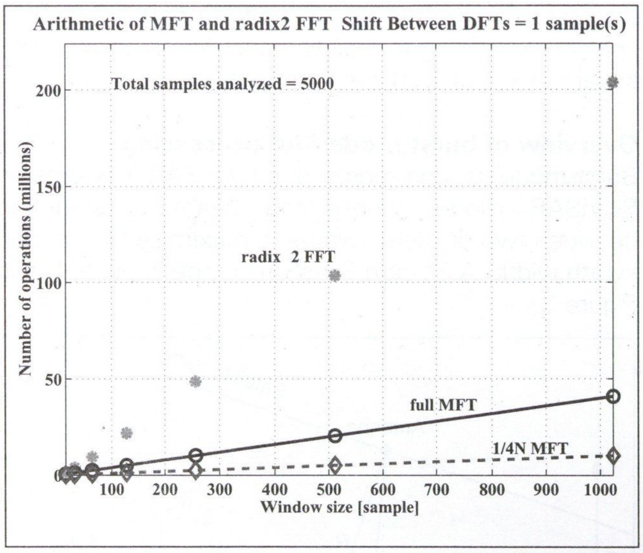


Figure 2 Arithmetic of MFT and Radix-2 FFT when qMFT = 1

The arithmetic of MFT is linear with the number of the computed spectrum coefficients N_c and the length of the data record M. For a given record size the MFT arithmetic remains the same, with varying shifts, while the FFT arithmetic drops down considerably as the value of shift gets larger.

The computational order of the MFT to recursively calculate the coefficients of an N-point DFT is N, a factor of log_2N improvement over the FFT. If only a subset of the spectrum components are needed, the computing load of the MFT can be further reduced, calculating only the frequency coefficients of interest. The MFT does not rely upon on N being power of two to obtain its efficiency, in contrast to standard FFT algorithms. In this way, the MFT can provide more efficient computation of the DFT when any or all of the following conditions apply:

- DFTs are highly overlapped
- only a few Fourier coefficients are needed
- a specific, non-composite DFT length is needed.

Concerning the above properties of the MFT, we can say that it can be useful in different applications of signal processing such as:

- on-line computations in real-time spectral analysis
- on-line signal identification and detection
- speech processing
- radar and sonar processing.

Application of MFT to burst-mode SAR data processing

Burst-mode operation is used in SAR systems, such as RADARSAT or ENVISAT, to image wide swaths, to save power or to reduce data link bandwidth. In this operational mode, the received data is windowed in a periodic fashion in the azimuth time variable, which results in a segmented frequency-time structure of its

Doppler energy. This frequency-time pattern requires special processing to maintain accurate focusing, consistent phase and efficient computing.

Overview of burst-mode SAR processing

Burst-mode is commonly used in SAR systems in ScanSAR mode, where the beam is switched between two or more swaths to maximize the imaged swath width. A 2-beam ScanSAR mode is illustrated in Figure 3.

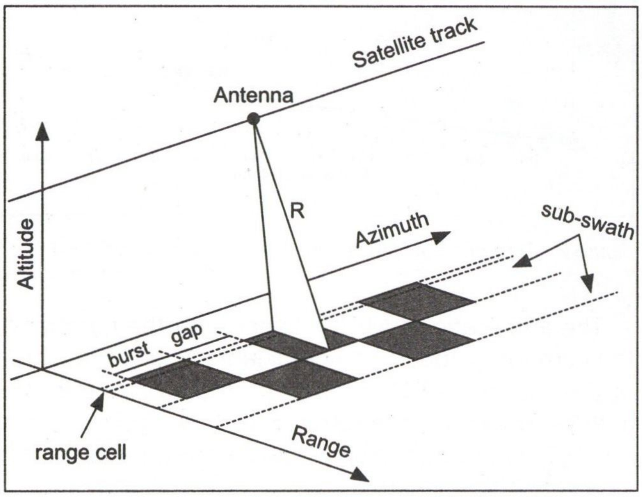


Figure 3 Burst-mode operation in 2-beam ScanSAR case

In this operation mode, the radar beam scans through one sub-swath for a certain time interval, and switches to the next one. After scanning through the second sub-swath, the radar switches back to the first one to start the next burst cycle. The burst cycle has to be short enough to make sure each target is fully exposed in at least one burst.

The data from one sub-swath have to be processed separately from other sub-swaths, because the radar beam covers a different ground area in different sub-swaths. In the azimuth direction, the data is segmented into discrete bursts (shaded area in Figure 3), while in range the signal of any sub-swath is continuous, thus the data is not acquired in discrete range bursts.

Properties of burst-mode processing

A typical 2-beam burst-mode data collection pattern is shown in Figure 4. Data from 16 consecutive, fully exposed targets in one range cell are shown, where the burst length is 20% of the aperture length. Dashed lines show the azimuth exposure time of each target if the SAR were operating in continuous mode, and the solid parts of each line show that part of each target actually exposed in burst mode. These are the valid targets of continuous-mode processing: they have complete frequency-time history and get compressed using the full Doppler aperture (F_a) matched-filter (e.g. in the RD algorithm).

The part of the target's exposure captured in burst mode varies with each target, which is illustrated in the frequency-time diagram of Figure 6. Each successive target is received at a lower Doppler frequency within a given burst, but is later captured at a higher frequency in the next burst, as long as it stays within the beam. The pulse repetition frequency (*PRF or* F_a) and the aperture length in azimuth time (T_a) are connected through the azimuth FM rate (K_a),

$$F_a = T_a K_a \text{ [Hz]}$$

In this example, T_a in the time-domain consist of 5 burst lengths (3 burst and 2 gaps), so F_a in the frequency-domain also consists of 5 burst bandwidths (Figure 4). Using eqn. (24), the synthetic aperture length in azimuth samples is

$$N_a = T_a F_a = \frac{F_a^2}{K_a}$$

Using the relationship between the time and the frequency domain given in eqn. (24), the shift between two consecutive targets' spectral energy (q_{tar}, Figure 4) can be obtained as follows:

$$q_{tar\,Hz} = T_{sampl} K_a = \frac{K_a}{F_a} \text{ [Hz]}$$

$$q_{tar\,bin} = round\left(\frac{q_{tar\,Hz}}{\Delta f}\right) = round\left(q_{tar\,Hz}\frac{N_{FFT}}{F_a}\right) =$$

$$= round\left(\frac{K_a N_{FFT}}{F_a^2}\right) \text{ [frequency bins]}$$

where T_{sampl} is the sampling time or the shift between two consecutive targets, Δf is one frequency bin in Hz and N_{FFT} is the length of the azimuth DFT in time samples. Note, q_{tar} is proportional to K_a and N_{FFT}, so the shift varies with range and the length of the DFT. The bandwidth of the burst in Hz and in frequency bins can be obtained using also eqn. (24):

$$F_{burst\,Hz} = T_{burst} K_a = \frac{N_b K_a}{F_a} \text{ [Hz]}$$

$$F_{burst\,\mathrm{bin}} = ceil\left(\frac{F_{burst\,Hz}}{\Delta f}\right) =$$

$$= ceil\left(\frac{N_b K_a N_{FFT}}{F_a^2}\right) \text{ [frequency bins]}$$

where N_b is the burst length in azimuth time samples.

The Doppler history of the 16 targets is also shown in Figure 4, where it is seen that it takes up to 2 bursts (e.g. burst 2 and 4) to cover all of them. The Doppler

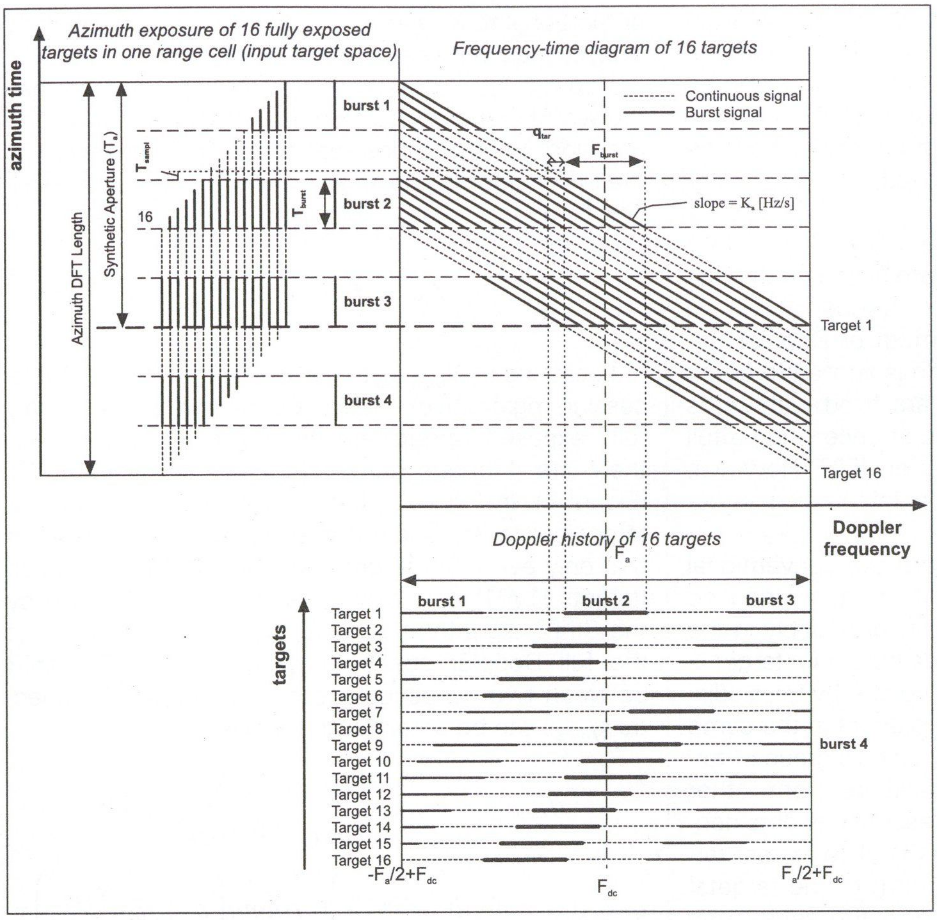


Figure 4 Burst-mode processing of 16 consecutive, evenly spaced and fully exposed target in one range cell

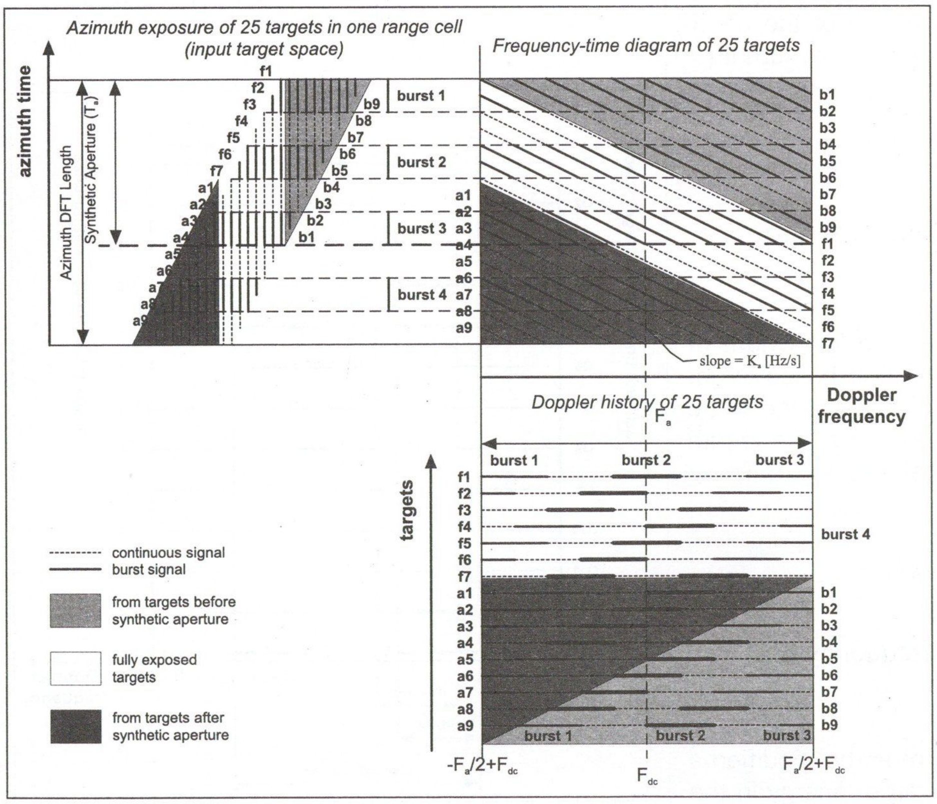


Figure 5 Burst-mode processing of 25 consecutive, evenly spaced, fully and partially exposed target in one range cell

history is the decomposition of the spectrum of targets after the matched filter multiplication. It shows the distribution of each target's spectral energy that would appear if a DFT was taken over the full 4 bursts and 4 gaps and than multiplied with the matched filter (MF). Note that the spectral energy distribution of targets is the same before and after the MF multiply, because the MF is the conjugate complex of the ideal target [3].

In the Doppler history, some targets appear in 2 full bursts (e.g. Target 6), some appear in 3 full bursts (e.g. Target 11), while others appear in two full and one partial burst. In this case, the average number of target exposures or bursts per aperture is 2.5. The number of bursts/aperture in ScanSAR systems is typically between 1.5 and 3.

Beside the fully captured targets, there are also partially exposed targets both at the leading edge and trailing edge of the azimuth DFT. These targets are incomplete, so they are discarded during continuous-mode processing.

The frequency-time diagram and Doppler history of partially exposed targets are shown in Figure 5. The light gray region corresponds to signals from targets that begin previous to the start of the DFT (targets b1-b9) and the dark gray region corresponds to signals from targets which end after the end of the DFT (targets a1-a9). Note that most of the partially exposed targets are also completely captured by one or two bursts, so they can be fully compressed using one burst width of their spectrum. In this way more targets with lower resolution can be fully compressed in the same synthetic aperture as in the continuous-mode for a given DFT length.

If single-look complex processing is to be done, then there is a choice of which bursts to use for each target. Normally, the target exposures closest to the Doppler centroid (F_{dc}) will be selected, as shown by the heavier lines in the Doppler history of Figure 4 and 5. However, other bursts may be chosen, when the data is processed for InSAR purposes.

The SIFFT Algorithm

Most SAR processing algorithms are based on the fast convolution principle where a frequency-domain matched filter is used in the azimuth or Doppler frequency domain. When this method is applied to burst-mode data, the inter-burst gaps are filled with zeros and all the bursts are compressed at once using a full length matched filter followed by an IFFT. However, the compressed targets are then left with a burst-induced modulation.

The SIFFT algorithm differs from the conventional fast convolution algorithm in that short, overlapped IFFTs are taken after the matched filter multiply in the Doppler domain [16]. So, when one burst of a target is fully captured by the IFFT, little or no energy from adjacent bursts of the same target is present in the same IFFT. In this way, each IFFT compresses a group of targets without interference (modulation) from other bursts, and an accurate impulse response is obtained. The IFFT is acting like a band-pass filter to extract target energy from the segmented form of the targets' spectra. The filter is time varying in the sense that each successive IFFT is applied to a different frequency band.

To capture a target fully, the length of the IFFT must be at least as long as the length of the bandwidth of one burst. Using eqn. (27) the minimum IFFT length is

$$N_{IFFT\,min} = F_{burst\,bin} =$$

$$= ceil\left(\frac{N_b K_a N_{FFT}}{F_a^2}\right) \text{[frequency bin]}$$

The IFFT cannot be longer than the bandwidth of one burst plus one gap, so that a fully-exposed target is not contaminated by a partial exposure of the same or another target at a different frequency. The length of the gap is equal to the burst length, so the maximum length IFFT is

$$N_{IFFT\,max} = 2F_{burst\,bin} =$$

$$= 2ceil\left(\frac{N_b K_a N_{FFT}}{F_a^2}\right) \text{[frequency bin]}$$

In practice, these length limits must be modified a little because of the spreading of target energy in the frequency domain, *i.e.* a guard band is used when locating the IFFTs. Note, $N_{IFFT\,max}$ and $N_{\,IFFT\,min}$ are proportional to K_a and N_{FFT}. The effect of this property is discussed in more details in [18].

Usually, $N_{IFFT\,max}$ is smaller than N_{FFT}, so less than the whole Doppler spectrum is used for azimuth compression, which means that the output resolution of the SIFFT algorithm is smaller than the maximum available by a factor of N_{IFFT}/N_{FFT}, thus

$$\rho_{SIFFT} = \rho_{\max}\frac{N_{IFFT}}{N_{FFT}}$$

Locations of $N_{IFFT\,min}$ to compress targets in the processing region (thick lines) are shown in Figure 6. Only fully exposed targets are shown in the case when there are 4 bursts and 4 gaps in the azimuth DFT (Figure 4). In Figure 6, both the input and the output target space are shown, from where it can be seen that only every 5th target from the input target space (targets *f*1-*f*61) gets compressed (targets O1-O13) by the SIFFT algorithm because the $N_{IFFT\,min}$ is 1/5th of the full Doppler spectrum ($\rho_{SIFFT} = 1/5$). The shift between two consecutive compressed targets' spectra (q_{outar}) can be obtained as follows,

$$q_{outar\,Hz} = q_{tar\,Hz}\frac{N_{FFT}}{N_{IFFT}} = \frac{K_a N_{FFT}}{F_a N_{IFFT}} \text{ [Hz]}$$

$$q_{outar\,bin} = round\left(\frac{q_{outar\,Hz}}{\Delta f}\right) = round\left(q_{outar\,Hz}\frac{N_{FFT}}{F_a}\right) =$$

$$= round\left(\frac{K_a N_{FFT}^2}{F_a^2 N_{IFFT}}\right) \text{[frequency bin]}$$

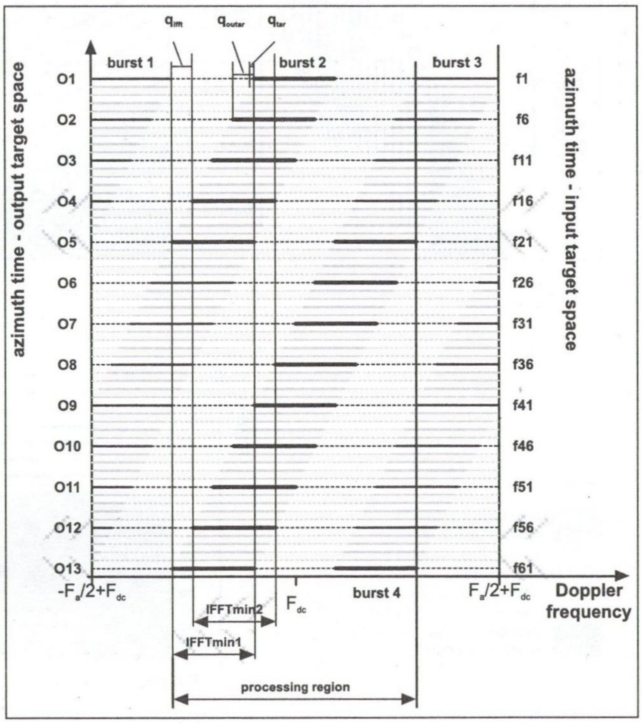


Figure 6 How minimum IFFTs are placed to compress fully exposed targets

It can be seen that *IFFT Min 1* captures the complete energy of a single burst spectra of targets *O5 (f21)* and *O13 (f61)*. For these targets, *IFFT Min 1* does not extract any energy from other bursts' spectra, so their impulse response is not corrupted by modulation. Similarly, *IFFT Min 2* captures the complete energy of a single burst spectra of targets *O4 (f16)* and *O12 (f56)*. In order to form a continuous output image, the results of successive IFFTs are stitched together [14]. If only bursts with the highest energy are used to compress targets, then each output target gets to a different output cell. Note, the first IFFT extracts targets with the highest indexes *(O5 and O13)* and as the IFFT is shifted towards higher frequencies in the Doppler spectrum, targets with lower indexes are compressed.

The shift between two consecutive IFFTs (q_{ifft}) is also indicated in Figure 6 and can be obtained as follows. All IFFTs start at the beginning of a burst's spectra of a target, so q_{ifft} can be divided into integer number of q_{outar} (Figure 7). The number of q_{outar} in the shift between two consecutive IFFTs is

$$Q_{outar} = floor\left(\frac{N_{IFFT} - F_{burst\,bin}}{q_{outar\,\mathrm{bin}}}\right) + 1$$

Using the equation above the shift between two consecutive IFFTs is

$$q_{ifft} = q_{outar\,bin}\left(floor\left(\frac{N_{IFFT} - F_{burst\,bin}}{q_{outar\,bin}}\right) + 1\right)$$
$$[\text{frequency bin}]$$

When $N_{IFFT\,Min}$ is used, the shift between IFFTs is equal to the shift between output targets ($q_{ifft} = q_{outar}$). When N_{IFFT} gets longer, q_{IFFT} also gets longer, thus fewer IFFTs are needed to compress all targets (i.e. one IFFT extracts more targets)

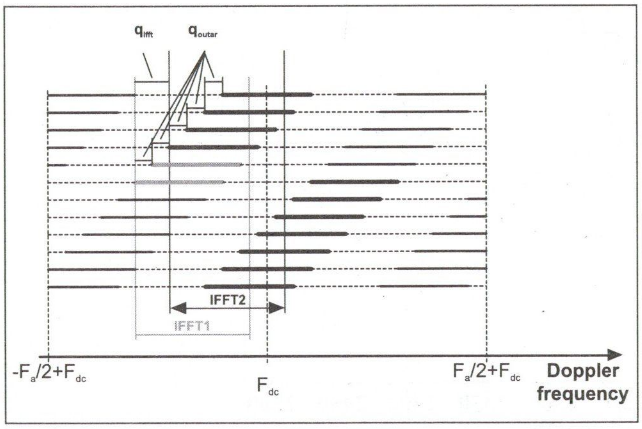


Figure 7 Shift between two consecutive IFFTs

Efficiency of SIFFT using the IMFT and the IFFT algorithms

Arithmetic of the SIFFT algorithm

The processing region of a burst-mode processing algorithm is three burst-bandwidth ($3F_{burst\ bin}$) long in the Doppler history (Figure 6). Thus both the IFFT and IMFT algorithms are applied only in this region when they are used in the SIFFT algorithm. It was shown in the previous section that there is q_{ifft} (eqn. (33)) shift between consecutive IFFTs, so the number of IFFTs applied in the processing region is

$$NUM_{IFFT} = ceil\left(\frac{3F_{burst\,bin} - N_{IFFT}}{q_{ifft}} + 1\right)$$

Than, the number of operations needed to compress all targets using the IFFT algorithm is

$$NOP_{IFFT} = NUM_{IFFT} \cdot NOP_{N_{IFFT}} =$$
$$= ceil\left(\frac{3F_{burst\,bin} - N_{IFFT}}{q_{ifft}} + 1\right) NOP_{N_{IFFT}}$$

where NOP_{NIFFT} is the number of real operations needed for one N sample long mixed-radix IFFT. Note if N is power of 2 (radix-2 IFFT) than $NOP_{NIFFT} = 5\,N\,log_2(N)$.

As we saw in Section 3.2, in case of the full-IMFT with a N_{IMFT} long window, $NOP_{NIFFT} = M(8N_{IMFT} + 2)$ (eqn. 24) real operations are needed to process an M-point complex data record. In the case of 2-beam burst processing $M = 3F_{burst\ bin}$, so the arithmetic of the IMFT algorithm is

$$NOP_{IMFT} = 3\,F_{burst\,\mathrm{bin}}\,(8\,N_{IMFT} + 2)$$

Note, both formulas in eqn. (35) and eqn. (36) depend on the azimuth DFT length (N_{FFT}) in the following way: NOP_{IFFT} through N_{IFFT}, $F_{burst\ bin}$ and q_{ifft}, while NOP_{IMFT} through N_{IMFT} and $F_{burst\ bin}$.

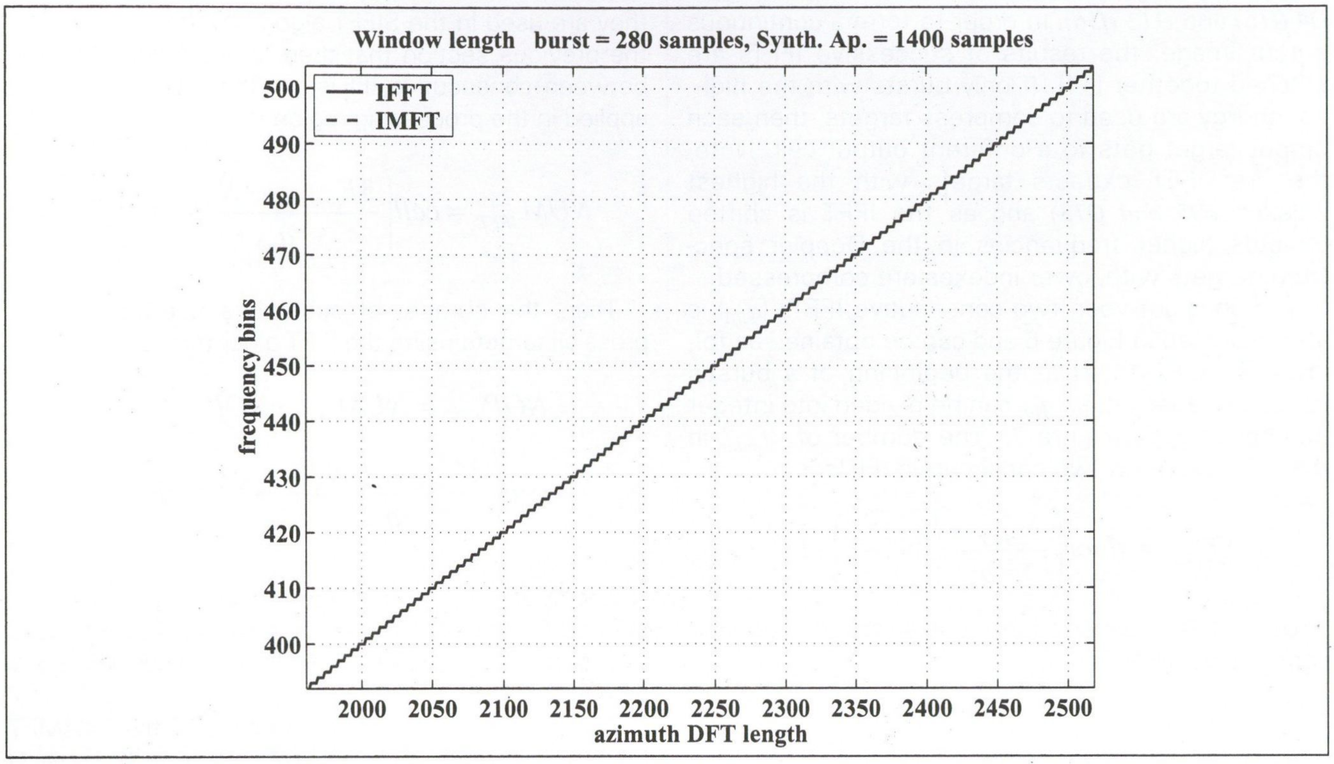
Processing parameter	Value	Unit
Azimuth sampling frequency (F_a)	1673.32	Hz
Azimuth FM rate (K_a)	-2000	Hz/s
Doppler Centroid (F_{dc})	447.1	Hz
Synthetic aperture length - 3 bursts-2 gaps (N_a)	1400	samples
Burst length (N_b)	280	samples
Points between equally spaced targets	135	samples
Output burst length (N_{outb})	56	samples

Table 1 Spaceborne SAR parameters assumed for SIFFT arithmetic calculation

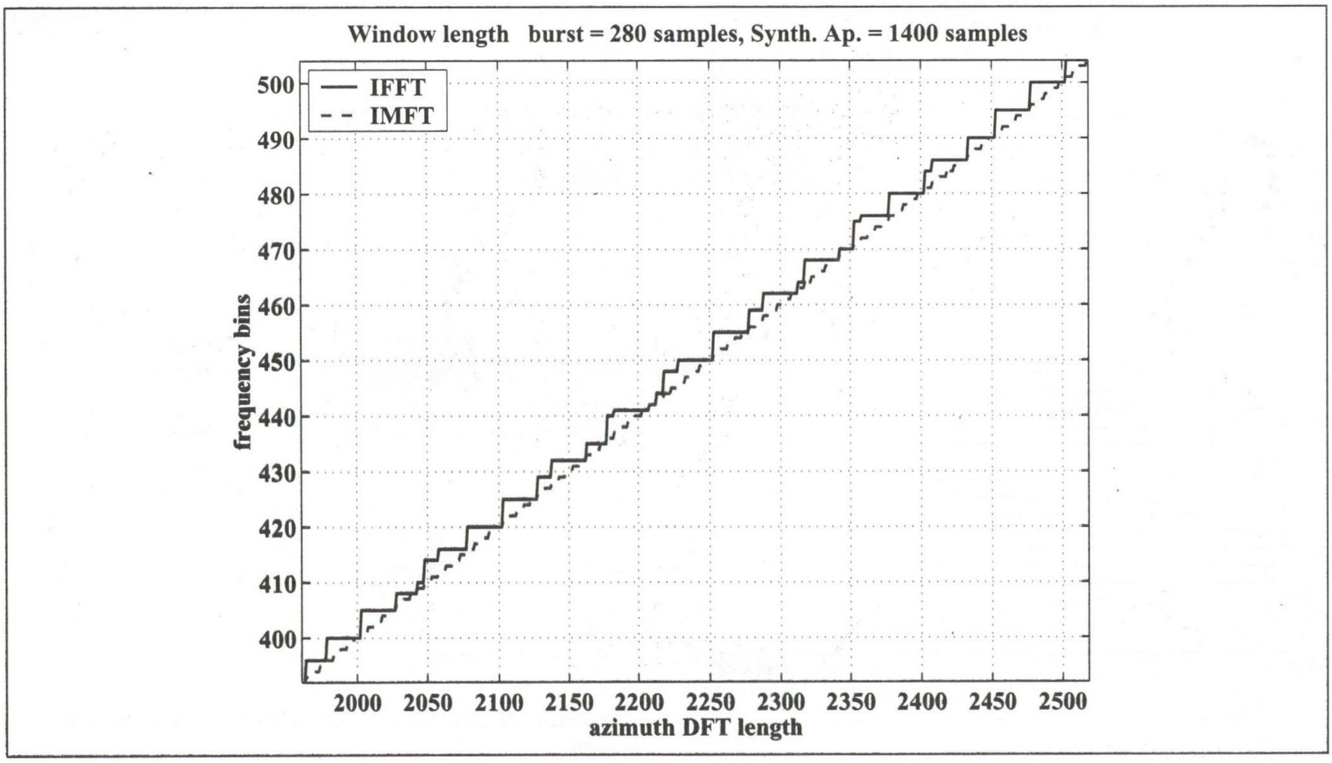
Efficiency of the SIFFT algorithm vs. azimuth DFT length

During the arithmetic calculation, radar parameters given in Table 1 are used with the following azimuth

DFT interval: 1960 ≤ N_{FFT} ≤ 2519. First, the arithmetic of the IFFT and IMFT algorithms vs. the azimuth DFT length, when the minimum IFFT lengths are used ($N_{IFFT} = N_{IMFT} = F_{burst\ bin}$) is given. Than the arithmetic of the case when the IFFT length is allowed to be up to 4 samples longer than the minimum (i.e. $F_{burst\ bin} \leq N_{IFFT} < F_{burst\ bin} + 4$ and $N_{IMFT} = F_{burst\ bin}$) is investigated. The later case allows some flexibility in choosing a favorable (more efficient) IFFT length from 5 window lengths, at the expense of a small decrease in SNR. More details on the relationship between SNR and IFFT window length are given in [14] and [15].



(a) minimum IFFT length



(b) 5 IFFT length to choose from

Figure 8 IMFT and IFFT window length vs. azimuth DFT length

Substituting the above given SAR parameters into eqn. (28) and (29), the window length of IMFT and IFFT can be obtained, thus $392 \leq N_{IMFT\ and} N_{IFFT} \leq 504$. In the first case (Figure 8 (a)) the window length of the IMFT and IFFT are the same and equal to the burst bandwidth. Note, all the values of the 113 long interval of the computed window lengths are used. In the second case, a favorable window size, larger than the minimum length can be chosen from 5 consecutive window length. The IMFT is more efficient when the window length is smaller, while the IFFT is more efficient when the window length is a higher composite number (e.g. the window length is power of two). It can be seen in Figure 8 (b) that the IFFT window is larger in most cases than the minimum window length, thus there are larger window sizes where the IFFT is more efficient. Note that in both cases, the signal processing system is rather complex if the IFFT algorithms are used, because all the different mixed-radix algorithms have to be implemented. In contrast, it is easier to implement the IMFT algorithm for variable burst and DFT length, because the same algorithm can be used for the different window length.

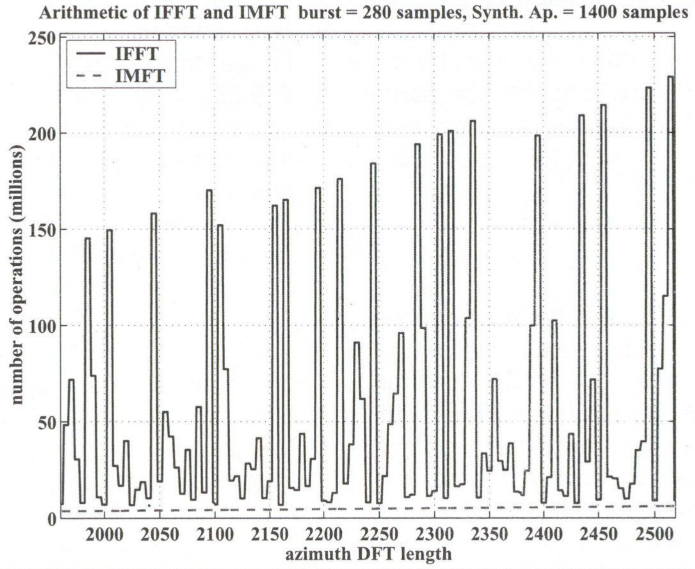


Figure 9 Arithmetic of the IFFT and IMFT algorithm vs. azimuth DFT, minimum IFFT length is used

The arithmetic of the IMFT and the IFFT algorithms for the two cases are given in Figure 9 and 10. It is seen from both figures that the arithmetic of the IFFT algorithm is quite variable depending upon the composition of the N_{IFFT} length. The IMFT arithmetic is much smoother and it is a quadratic function of the azimuth DFT length, (eqn. (38), $N_{IMFT} = F_{burst}$). It is also seen from figures that the IMFT algorithm is more efficient in both cases, even if there is an option to choose a more suitable window length for the IFFT algorithm (Figure 10).

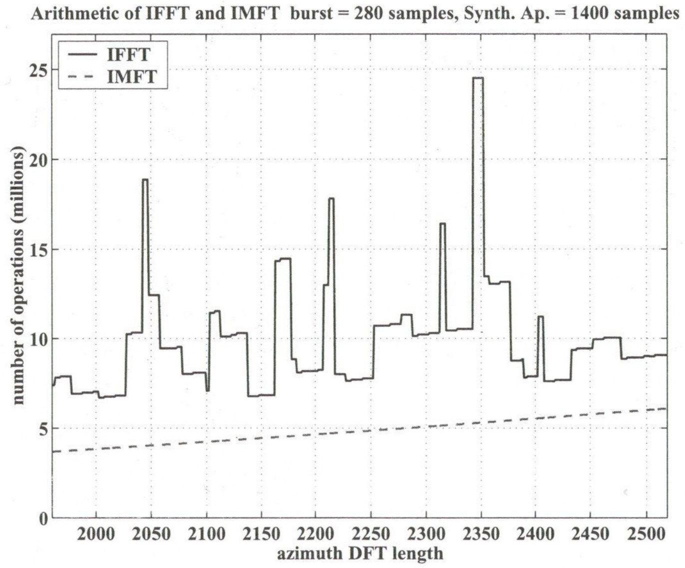


Figure 10 Arithmetic of the IFFT and IMFT algorithm vs. azimuth DFT, 5 IFFT length to choose from

From the above given arithmetic surveys it can be seen that the IMFT algorithm can improve the computational efficiency of the SIFFT algorithm and has the following advantages when it is applied to the SIFFT algorithm:

- For a given azimuth DFT length, the IMFT algorithm is most efficient when $N_{IMFT\,min}$ (i.e. the burst bandwidth) is used. So, beside the efficiency targets with maximum SNR are compressed.
- The IMFT arithmetic is smooth and it is a quadratic function of the azimuth DFT length opposite to the arithmetic of the IFFT algorithm which is quite variable depending upon the composition of the window length.
- It is easier to implement the IMFT algorithm for different burst and N_{FFT} lengths, because the same IMFT algorithm can be used for the different window lengths.

Conclusions

The momentary matrix transform has been introduced and it has been shown that, when it takes the form of the DFT or the IDFT, the resulting MFT/IMFT have an efficient recursive computational structure. The coefficients of the MFT/IMFT can be calculated independently and only one complex multiplication and two complex additions are needed to update each spectrum component. This is a factor of $\log_2(N)$ improvement over the radix-2 FFT algorithm if all incremental DFT results are needed. The efficiency of the MFT/IMFT does not rely upon the transform length being a power of two, in contrast to standard FFT algorithms.

In burst-mode SAR processing, the time-varying spectral properties of the azimuth received data requires that highly-overlapped inverse DFTs be used at specific locations in the frequency domain to obtain accurate azimuth compression. Detailed description of the properties of the SIFFT algorithm was given and it was shown that the IMFT can be more efficient than the IFFT when it is applied to the SIFFT burst-mode data processing algorithm, especially when the highest possible SNR is desired.

References

1. A. Papoulis, *Signal Analysis*. McGraw-Hill, 1977
2. G. Strang, *Linear Algebra and Its Applications*. Saunders College Publishing, Third Edition, 1988
3. J. Curlander and R. McDonough, *Synthetic Aperture Radar: System and Signal Processing*. *Wiley*, New York, 1991.
4. J. G. Proakis and D.G. Manolakis, *Digital Signal Processing*. Prentice Hall, Third Edition, 1996
5. R. R. Bitmead and B. D. O. Anderson, „Adaptive frequency sampling filters," *IEEE Trans. On Circuits and Systems*, vol. CAS-28, pp. 524-534, June 1981.
6. J. Dudás, *The Momentary Fourier Transform*. Ph.D. thesis, Technical University of Budapest, 1986.
7. H. Lilly, "Efficient DFT-based model reduction for continuous systems", *IEEE Trans. on Automatic Control*, vol.36, pp. 1188-1193, Oct. 1991.
8. B. G. Sherlock and D. M. Monro, "Moving discrete Fourier transform", *IEE Proceedings-F*, vol. 139, pp. 279-282, Aug. 1992.
9. S. Albrecht, I. Cumming and J. Dudás, "The momentary Fourier transformation derived from recursive matrix transformations", in *Proceedings of the 13th International Conference on Digital Signal Processing, DSP'97*, (Santorini, Greece) vol. 1, pp. 337-340, July, 1997.
10. K. Tomiyasu, "Tutorial Review of Synthetic-Aperture Radar (SAR) with Applications to Imaging of Ocean Surface, *Proceedings of IEEE*, Vol. 66, No. 5, pp. 563-583, May 1978.
11. I. Cumming Y. Guo and F. Wong, "Analysis and Precision Processing of Radarsat ScanSAR Data", *In Geomatics in the Era of Radarsat, GER'97*, (Ottawa, Canada), May 25-30, 1997.
12. F. Wong, D. Stevens and I. Cumming, "Phase-Preserving Processing of ScanSAR Data with Modified Range Doppler Algorithm", in *Proceedings of the International Geoscience and Remote Sensing Symposium, IGARSS'97*, (Singapure), pp.725-727, August 3-8, 1997.
13. I. Cumming Y. Guo and F. Wong, "A Comparison of Phase-Preserving Algorithms for Burst-mode ScanSAR Data Processing", in *Proceedings of the International Geoscience and Remote Sensing Symposium, IGARSS'97*, (Singapure), pp.731-733, August 3-8, 1997.
14. I. Cumming Y. Guo and F. Wong, "Modifying the RD Algorithm for Burst-mode SAR Processing", in *Proceedings of the European Conference on Synthetic Aperture Radar, EUSAR'98*, (Friedrichshafen, Germany), pp.477-480, May 25-27, 1998.
15. S. Albrecht and I. Cumming, "Application of Momentary Fourier Transform to SAR Processing", *IEE Proceedings: Radar, Sonar and Navigation*, 146(6), pp. 285-297, December 1999.

Contents

THEORETICAL BACKGROUNDS

MOBILE SYSTEMS

TRAFFIC ROUTING