

UTILIZAREA REPREZENTĂRIILOR TIMP-FRECVENȚĂ ÎN ANALIZA FENOMENELOR NESTAȚIONARE

Teză destinată obținerii
titlului științific de doctor inginer
la
Universitatea "Politehnica" din Timișoara
în domeniul Inginerie Electronică și Telecomunicații
de către:

as. ing. Sălăgean Marius Ioan

Conducător științific:	prof.univ.dr.ing. Ioan Naforniță
Referenți științifici:	prof.univ.dr. Monica Borda
	prof.univ.dr.ing. Corneliu Rusu
	conf.univ.dr.ing. Alexandru Isar

Ziua susținerii tezei: 11.03.2011

Seriile Teze de doctorat ale UPT sunt:

- | | |
|------------------------|---|
| 1. Automatică | 7. Inginerie Electronică și Telecomunicații |
| 2. Chimie | 8. Inginerie Industrială |
| 3. Energetică | 9. Inginerie Mecanică |
| 4. Ingineria Chimică | 10. Știința Calculatoarelor |
| 5. Inginerie Civilă | 11. Știința și Ingineria Materialelor |
| 6. Inginerie Electrică | |

Universitatea „Politehnica” din Timișoara a inițiat seriile de mai sus în scopul diseminării expertizei, cunoștințelor și rezultatelor cercetărilor întreprinse în cadrul școlii doctorale a universității. Seriile conțin, potrivit H.B.Ex.S Nr. 14 / 14.07.2006, tezele de doctorat susținute în universitate începând cu 1 octombrie 2006.

Copyright © Editura Politehnica – Timișoara, 2006

Această publicație este supusă prevederilor legii dreptului de autor. Multiplicarea acestei publicații, în mod integral sau în parte, traducerea, tipărirea, reutilizarea ilustrațiilor, expunerea, radiodifuzarea, reproducerea pe microfilme sau în orice altă formă este permisă numai cu respectarea prevederilor Legii române a dreptului de autor în vigoare și permisiunea pentru utilizare obținută în scris din partea Universității „Politehnica” din Timișoara. Toate încălcările acestor drepturi vor fi penalizate potrivit Legii române a drepturilor de autor.

România, 300159 Timișoara, Bd. Republicii 9,
tel. 0256 403823, fax. 0256 403221
e-mail: editura@edipol.upt.ro

Cuvânt înainte

Teza de doctorat a fost elaborată pe parcursul activității mele în cadrul Departamentului de Comunicații al Facultății de Electronică și Telecomunicații a Universității „Politehnica” din Timișoara.

Finalizarea ei se datorează într-o bună măsură și persoanelor menționate mai jos, cărora le adresez gratitudinea mea.

Primul meu cuvânt de mulțumire se îndreaptă înspre conducătorul meu de doctorat, domnul prof. dr. ing. Ioan Naforniță. Datorită sfaturilor dânsului, m-am îndreptat înspre acest domeniu de cercetare, iar finalizarea acestei lucrări nu ar fi fost posibilă fără suportul științific și moral de care m-am bucurat în mod constant din partea dânsului pe întreaga durată a tezei. Îi datorez un sincer cuvânt de mulțumire și recunoștință pentru faptul de a mă fi cooptat în colectivul Departamentului de Comunicații cu mulți ani în urmă.

Țin de asemenea să le mulțumesc referenților științifici ai tezei, doamna prof. dr. ing. Monica Borda, și domnului prof. dr. ing. Corneliu Rusu, pentru timpul pe care l-au dedicat analizei acestei lucrări, și pentru efortul pe care l-au făcut pentru a lua parte la susținerea publică a tezei.

În particular, doresc să îmi exprim gratitudinea față de domnul prof. dr. ing. Alexandru Isar, pentru sfaturile științifice primite de-a lungul acestor ani care m-au ajutat la finalizarea acestei teze.

Un sincer cuvânt de mulțumire și recunoștință datorez doamnei prof. dr. ing. Miranda Naforniță pentru încurajări și sprijinul necondiționat.

Îi mulțumesc domnului decan al Facultății de Electronică și Telecomunicații, domnul prof. dr. ing. Marius Oteșteanu, pentru acceptul de a prezida comisia de doctorat și pentru susținerea materială constantă de care m-am bucurat din partea decanatului facultății noastre, care mi-a permis participarea la mai multe conferințe din țară.

Adresez calde și sincere mulțumiri domnului prof. dr. André Quinquis și domnului dr. Cornel Ioana pentru oportunitatea de a efectua un stagiu de cercetare la “Ecole Nationale Supérieure des Ingénieurs des Etudes des Techniques d’Armement – ENSIETA” din Brest, Franța.

Nu în ultimul rând doresc să mulțumesc familiei mele și tuturor prietenilor pentru că au fost mereu aproape de mine.

Timișoara, martie 2011

Sălăgean Marius Ioan

Soției, fiicei și mamei mele

Sălăgean, Ioan Marius

Utilizarea reprezentărilor timp-frecvență în analiza fenomenelor nestaționare

Teze de doctorat ale UPT, Seria 7, Nr. 34, Editura Politehnica, 2011, 116 pagini, 52 figuri, 27 tabele.

ISSN: 1842-7014

ISBN: 978-606-554-267-9

Cuvinte cheie: semnale nestaționare, reprezentări timp-frecvență, undișoare, frecvență instantanee, securitatea rețelilor
Rezumat:

Scopul principal al tezei este de a propune și studia metode timp-frecvență adaptate semnalelor întâlnite în realitate și de a sublinia potențialul acestor metode în câteva aplicații practice. Atenția este focalizată asupra recunoașterii modulației multi-purtătoare și mono-purtătoare, îmbunătățirii performanțelor de estimare a frecvenței instantanee a metodei de prelucrare timp-frecvență ce utilizează operatori morfologici (TFR-MO), analiza unui algoritm de determinare a celei mai bune undișoare mamă bazat pe teoria polinoamelor, util pentru compresia semnalelor și dezvoltării unui sistem complet de detecție a anomaliilor de rețea, bazat pe transformarea wavelet staționară analitică (ASWT) și pe cumulantul de ordinul patru (Cum4).

CUPRINS

Abrevieri.....	1
Lista tabelor.....	3
Lista figurilor.....	4
Introducere.....	6
1. Reprezentări timp-frecvență (RTF).....	8
1.1. RTF liniare.....	8
1.1.1. Transformarea Fourier Scurtă (STFT).....	8
1.1.2. Transformarea Wavelet (WT).....	9
1.2. RTF biliniare.....	10
1.2.1. Distribuția Wigner-Ville (WVD).....	10
1.3. RTF bazate pe modelarea polinomială a fazei semnalelor.....	11
1.3.1. Caracterizarea polinomială a fazei.....	11
1.3.2. Reducerea ordinului polinomial cu ajutorul tehnicii de deformare. Metoda "WarpComp".....	13
2. Aplicații ale RTF pentru semnale cu fază polinomială.....	15
2.1. Recunoașterea modulațiilor multi-purtătoare bazată pe metoda WarpComp.....	15
2.1.1. O privire generală asupra semnalelor de comunicații.....	15
2.1.2. Principiul de identificare a modulațiilor numerice.....	16
2.1.3. Rezultate.....	18
3. Estimarea frecvenței instantanee bazată pe tehnici de prelucrare a imaginii.....	23
3.1. Considerații privind împrăștierea zgomotului în planul timp-frecvență.....	23
3.2. Rolul operatorilor matematici morfologici.....	25
3.3. Metoda RTF ce utilizează operatori morfologici în estimarea IF (TFR-MO).....	27
3.4. Studiul performanțelor TFR-MO.....	28
3.4.1. Semnale mono-componentă.....	28
3.4.2. Semnale multi-componente.....	36
3.5. Îmbunătățirea performanțelor TFR-MO.....	37
3.6. Concluzii.....	41
4. Determinarea celei mai bune undișoare mamă bazat pe teoria polinoamelor.....	42
4.1. Legătura dintre undișoarele mamă și funcțiile polinomiale.....	42
4.2. Algoritmul DWT de estimare a gradului unui polinom.....	45
4.2.1. Implementare.....	45
4.2.2. Evaluarea performanțelor pentru câteva tipuri de semnale.....	46
4.2.3. Efectul filtrării coeficienților wavelets de detaliu diferiți de zero.....	50
4.2.4. Influența numărului de eșantioane din semnal.....	55
5. Aplicații ale RTF în detecția anomaliilor din traficul de rețea.....	58
5.1. Introducere.....	58
5.2. Caracteristici ale IDS-urilor.....	60
5.3. Metode de detecție.....	62
5.3.1. Detecția bazată pe semnătură.....	62
5.3.2. Detecția bazată pe anomalii.....	63
5.4. Tipuri de date colectate.....	64
5.4.1. Date specifice sistemului.....	64

5.4.2. Date specifice aplicației.....	64
5.4.3. Date specifice rețelei.....	65
5.5. Tipuri de atacuri.....	65
5.6. Considerații privind îmbunătățirea performanțelor IDSs.....	72
5.7. Utilizarea analizei wavelet în detecția anomaliilor.....	73
5.8. Arhitectura generală a sistemului de detecție.....	76
5.8.1. Analiza traficului de rețea.....	76
5.8.2. Analiza Wavelet.....	78
5.8.3. Analiza statistică (Cum4) și detecția.....	80
5.9. Analiza performanțelor de detecție a anomaliilor.....	82
5.9.1. Parametrii de simulare și mărimile de evaluare a performanțelor	82
5.9.2. Rezultatele detecției la diferite scări	85
5.9.3. Alegerea undișoarei mamă.....	98
5.9.4. Influența lungimii ferestrei de detecție.....	100
5.9.5. Alegerea pragurilor de decizie.....	101
5.10. Concluzii.....	102
6. Contribuții și concluzii.....	103
Anexa 1.....	106
Anexa 2.....	108
Bibliografie.....	110

ABREVIERI

AM	Amplitude Modulation
ARX	AutoRegressive with eXogenous
ASK	Amplitude Shift Keying
ASWT	Analytical Stationary Wavelet Transform
CTD	Complex Time Distribution
Cum4	Cumulant de ordinul 4
CWC	Cumulant Wavelet Coefficients Signal
CWT	Continuous Wavelet Transform
DARPA	Defense Advanced Research Projects Agency
DAVB	Digital Audio and Video Broadcasting
DNS	Domain Name System
DoS	Denial of Service
DWT	Discrete Wavelet Transform
FM	Frequency Modulation
FSK	Frequency Shift Keying
FT	Fourier Transform
FTJ	Filtru Trece Jos
FTP	File Transfer Protocol
FTS	Filtru Trece Sus
GMM	Gaussian Mixture Model
GT	Gabor Transform
HAF	High Ambiguity Function
HIDSs	Host Intrusion Detection Systems
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IDSs	Intrusion Detection Systems
IDWT	Inverse Discrete Wavelet Transform
IF	Instantaneous Frequency
IP	Internet Protocol
IPSec	Internet Protocol Security
LRU	Least Recently Used
MIME	Multipurpose Internet Mail Extensions
ml-HAF	Multi Lag High Ambiguity Function
ml-PHAF	Multi Lag Multiplicative High Ambiguity Function
MSE	Mean Square Error
NIDSs	Network Intrusion Detection Systems

2 ABREVIERI

OFDM	Orthogonal Frequency Division Multiplexing
PPS	Polynomial Phase Signal
PSK	Phase Shift Keying
QPSK	Quadrature Phase Shift Keying
RdI	Regiune de Interes
RTF	Reprezentare Timp-Frecvență
S4Z1	Săptămâna 4, Ziua 1
SNR	Signal to Noise Ratio
SSH	Secure Shell
SSL	Secure Socket Layer
STFT	Short Time Fourier Transform
SWT	Stationary Wavelet Transform
TCP	Transmission Control Protocol
TFR-MO	Morphology Operators based Time-Frequency Representation
TFR-IMO	Improved Morphology Operators based Time-Frequency Representation
UDP	User Datagram Protocol
VPN	Virtual Private Network
VWC	Variance Wavelet Coefficients Signal
WADeS	Wavelet-based Attack Detection Signatures
WiMAX	Worldwide Interoperability for Microwave Access
WOFDM	Wavelet-based OFDM
WPT	Wavelet Packet Transform
WT	Wavelet Transform
WVD	Wigner-Ville Distribution

LISTA TABELELOR

2.1	Performanțele privind numărul de purtătoare detectate, $N=3$ niveluri și 100 semnale OFDM.....	
2.2	Performanțele privind numărul de purtătoare detectate, $N=3$ niveluri și 100 semnale QPSK.....	
2.3	Parametrii semnalelor de test din baza de date COMINT și a bateriilor de filtre utilizate.....	
3.1	MSE al IF estimate, exemplul 1.....	
3.2	MSE al IF estimate, exemplul 2.....	
3.3	MSE al IF estimate cu metoda TFR-MO și TFR-IMO, exemplul 2.....	
4.1	Parametrii de simulare a semnalelor de test utilizate în evaluarea performanțelor DWT de reconstrucție.....	
4.2	Performanțele de aproximare pentru metoda DWT pentru semnalelor de test din tabelul 4.1.....	
4.3	Selecție a performanțelor de aproximare a semnalului de test S_9 , pentru diferite praguri de filtrare	
4.4	Selecție a performanțelor de aproximare a semnalului de test S_{11} , pentru diferite praguri de filtrare	
4.5	Selecție a performanțelor de aproximare a semnalului de test S_{12} , pentru diferite praguri de filtrare	
4.6	Performanțele de aproximare pentru semnalul S_8 , în funcție de numărul de eșantioane disponibile din semnal	
4.7	Performanțele de aproximare pentru semnalul S_{11} , în funcție de numărul de eșantioane disponibile din semnal	
5.1	Mărimi caracteristice ale traficului de rețea	
5.2	Parametrii tipurilor de anomalii din S4Z1, $T_s=1$ minut	
5.3	Parametrii de simulare utilizați pentru evaluarea performanțelor de detecție	
5.4	Performanțele de detecție ale anomaliilor pentru S4Z1, la scara $J=1$	
5.5	Performanțele de detecție ale anomaliilor pentru S4Z1, la scara $J=2$	
5.6	Performanțele de detecție ale anomaliilor pentru S4Z1, la scara $J=3$	
5.7	Performanțele de detecție ale anomaliilor pentru S4Z1, la scara $J=4$	
5.8	Performanțele de detecție ale anomaliilor pentru S4Z1, la scara $J=5$	
5.9	Performanțele de detecție ale anomaliilor obținute prin corelarea rezultatelor mai multor scări, pentru S4Z1	
5.10	Performanțele de detecție ale anomaliilor pentru S4Z1, cu undișoarele Daubechies, la scara $J=1$	
5.11	Performanțele de detecție ale anomaliilor pentru S4Z1, cu undișoarele Coiflet, la scara $J=1$	
5.12	Performanțele de detecție ale anomaliilor pentru S4Z1, cu undișoarele Symmlet, la scara $J=1$	
5.13	Performanțele de detecție ale anomaliilor pentru S4Z1, pentru diferite lungimi L_{det} , la scara $J=1$	
5.14	Performanțele de detecție ale anomaliilor pentru S4Z1, pentru diferite praguri de decizie, la scara $J=1$	

LISTA FIGURILOR

- 1.1 Pavajul timp-frecvență: Shannon (a) Fourier (b) și STFT (c)
- 1.2 Partajarea planului timp-frecvență pentru WT
- 1.3 Operatorii de descompunere și de reconstrucție în analiza multirezoluție
- 1.4 Termenii de interferență a WVD
- 1.5 Algoritmii de estimare a coeficienților polinomiali
- 1.6 Reducerea ordinului polinomial bazată pe operatorul de deformare
- 2.1 Schema bloc generală de prelucrare pentru identificarea modulației OFDM
- 2.2 Exemplu de modulație multi-purtătoare
- 2.3 Caracteristica de frecvență a filtrelor de tip Cebâșev II, pentru $N=3$ niveluri de descompunere
- 2.4 Exemplu de modulație QPSK
- 2.5 Arborele de descompunere rezultat pentru un semnal multi-purtătoare din baza de date COMINT
- 2.6 Arborele de descompunere rezultat pentru semnalul FSK din baza de date COMINT
- 3.1 Efectul operatorului de dilatare asupra imaginilor
- 3.2 Efectul operatorului de scheletizare asupra imaginilor
- 3.3 Metoda timp-frecvență de estimare IF bazată pe operatori morfologici (TFR-MO)
- 3.4 Semnal SFP cu amplitudine constantă, cu zgomot gaussian, $SNR=3dB$, exemplul 1
- 3.5 Estimarea IF prin metoda TFR-MO, exemplul 1
- 3.6 Comparatie între TRF-MO și câteva reprezentări timp-frecvență, exemplul 1
- 3.7 Performanțele MSE al IF în raport cu SNR, exemplul 1
- 3.8 Semnal SFP cu amplitudine constantă, cu zgomot gaussian, $SNR=3dB$, exemplul 2
- 3.9 Estimarea IF prin metoda TFR-MO, exemplul 2
- 3.10 Comparatie între TRF-MO și câteva reprezentări timp-frecvență, exemplul 2
- 3.11 Performanțele MSE al IF în raport cu SNR, exemplul 2
- 3.12 Semnal multi-component cu amplitudine constantă, cu zgomot gaussian, $SNR=30dB$
- 3.13 Estimarea IF prin metoda TFR-MO, semnal multi-component
- 3.14 Segmentarea suportului semnalului analizat
- 3.15 Estimarea IF prin metoda TFR-IMO, $SNR=30dB$, exemplul 2
- 3.16 Estimarea IF prin metoda TFR-IMO, $SNR=3dB$, exemplul 2
- 3.17 Performanțele MSE al IF în raport cu SNR
- 4.1 Semnal polinomial (a), numărul de detalii nule a undișoarelor (b), eroarea MSE de aproximare în funcție de gradul polinomial de interpolare (c) și în funcție de numărul de momente nule a undișoarelor (d)
- 4.2 Algoritmii DWT de estimare a gradului polinomului ce aproximează un semnal
- 4.3 Semnalul S_9 reconstruit utilizând undișoara Daubechies18, cu $N_d = 2$ (a), și $N_d = 7$ (b)
- 4.4 Semnalul S_{11} reconstruit utilizând undișoara Daubechies20, $N_d = 2$ (a), și Daubechies12, $N_d = 15$ (b)
- 4.5 Semnalul S_{12} reconstruit utilizând undișoara Daubechies12, $N_d = 63$, în

- intervalul [1, 128] (a), și în intervalul [60, 80] (b)
- 4.6 Numărul de detalii nule a undișoarelor (a), eroarea MSE de în funcție de numărul de momente nule a undișoarelor (b), pentru semnalul S_8 cu $N=32,64,128$ eşantioane
- 4.7 Numărul de detalii nule a undișoarelor (a), eroarea MSE de în funcție de numărul de momente nule a undișoarelor (b), pentru semnalul S_{11} cu $N=64,128,512$ eşantioane
- 5.1 Arhitectura generală sistemului de detecție a anomaliilor
- 5.2 Blocul de analiză a traficului de rețea
- 5.3 Implementarea SWT folosind bancuri de filtre
- 5.4 Implementarea ASWT
- 5.5 Semnal de trafic care conține 2 anomalii în $t=200$ și $t=400,401$
- 5.6 Semnalul VWC rezultat pentru semnalul de trafic din figura 5.5
- 5.7 Semnalul CWC rezultat pentru semnalul de trafic din figura 5.5
- 5.8 Numărul de fluxuri (a) TCP, (b) UDP și (c) ICMP într-un minut, pentru S4Z1
- 5.9 Rezultatul detecției pentru S4Z1, la scara $J=1$, pentru M_8 , cu Daubechies-8, $L_{det}=26$, $\alpha=2$
- 5.10 Rezultatul detecției pentru S4Z1, la scara $J=2$, pentru M_1 , cu Daubechies-4, $L_{det}=30$, $\alpha=1$
- 5.11 Rezultatul detecției pentru S4Z1, la scara $J=3$, pentru M_{11} , cu Symmlet-5, $L_{det}=28$, $\alpha=3$
- 5.12 Rezultatul detecției pentru S4Z1, la scara $J=4$, pentru M_{14} , cu Symmlet-5, $L_{det}=2$, $\alpha=3$
- 5.13 Rezultatul detecției pentru S4Z1, la scara $J=5$, pentru M_2 , cu Daubechies-4, $L_{det}=24$, $\alpha=1$
- 5.14 Performanța F_s (a) și P_s/F_s corespunzătoare (b), pe cele 5 scări
- 5.15 Performanța P_s (a) și P_s/F_s corespunzătoare (b), pe cele 5 scări
- 5.16 Performanțele P_s/F_s (a) și $1/2 (DR_2 + P_s/F_s)$ (b), pe cele 5 scări

INTRODUCERE

Scopul principal al tezei este de a propune și studia metode timp-frecvență adaptate semnalelor întâlnite în realitate și de a sublinia potențialul acestor metode în câteva aplicații practice. Nu există nici un domeniu de aplicare a teoriei semnalelor în care să nu existe aplicații ale reprezentărilor timp-frecvență. De fapt, fiecare metodă de acest tip a apărut din nevoia rezolvării unei probleme practice. Cu scopul de a răspunde obiectivelor de mai sus, teza este structurată după cum urmează.

În capitolul 1 sunt prezentate metodele timp-frecvență clasice: liniare (STFT, WT) și biliniare (WVD), cu avantajele și limitările lor. Tot în cadrul acestui capitol sunt prezentate câteva din reprezentările timp-frecvență bazate pe modelarea polinomială a fazei semnalelor.

În capitolul al doilea este prezentată o metodă de recunoaștere a modulației multi-purtătoare și mono-purtătoare bazată pe metoda "WarpComp", o reprezentare timp-frecvență bazată pe modelarea polinomială a fazei semnalelor. Metoda propusă reprezintă o contribuție personală. În final sunt prezentate rezultatele obținute în urma simulărilor.

Capitolul 3 este dedicat estimării frecvenței instantanee folosind o metodă de prelucrare timp-frecvență ce utilizează operatori morfologici, denumită în teză TFR-MO. Au fost analizate și comparate performanțele acestei metode pentru semnale mono-componentă și multi-componente, cu un comportament puternic nestaționar. Această analiză reprezintă o contribuție personală. Apoi, am propus o nouă implementare a metodei TFR-MO (TFR-IMO), bazată pe un algoritm secvențial de prelucrare, cu scopul de a îmbunătăți performanțele de estimare a metodei TFR-MO pentru semnale cu frecvența instantanee puternic neliniară. Rezultatele obținute sunt o contribuție personală.

În capitolul 4 am analizat un algoritm de determinare a celei mai bune undișoare mamă bazat pe teoria polinoamelor, util în compresia semnalelor. Am făcut, de asemenea, o analiză experimentală detaliată a performanțelor de aproximare a metodei propuse și am studiat influența filtrării coeficienților wavelet de detaliu diferiți de zero precum și influența numărului de eşantioane din semnal. Rezultatele prezentate și discutate în acest capitol reprezintă o contribuție personală.

Capitolul 5 debutează cu prezentarea celor mai importante caracteristici ale sistemelor de detecție a intruziunilor (IDS): acuratețe, eficiență, performanță, securitate, scalabilitate. Apoi, sunt introduse cele două tipuri de metode de detecție: bazată pe semnătură și bazată pe anomalii. După evidențierea avantajelor și dezavantajelor acestor metode de detecție, se trec în revistă principalele tipuri de date cu care lucrează sistemele IDS. Pentru dezvoltarea unor sisteme IDS performante și eficiente, este importantă cunoașterea cât mai bună a atacurilor existente și a tehnicilor utilizate în acest scop. Prin urmare, o bună parte din acest

capitol este consacrată descrierii acestor atacuri. În continuare sunt prezentate unele considerații privind îmbunătățirea performanțelor IDS. Urmează apoi sistemul complet de detecție a anomaliilor de rețea propus, bazat pe transformarea wavelet staționară analitică (ASWT) și pe cumulantul de ordinul patru (Cum4). Acest sistem de detecție a anomaliilor reprezintă o contribuție personală. În paragraful 5.9 am făcut o analiză experimentală detaliată a performanțelor de detecție a anomaliilor. Rezultatele prezentate și discutate în acest capitol reprezintă o contribuție personală.

În capitolul 6 sunt trecute în revistă contribuțiile personale, și, legate de acestea, concluziile tezei.

1. REPREZENTĂRI TIMP-FRECVENȚĂ (RTF)

1.1. RTF liniare

O reprezentare este liniară dacă rezultatul aplicării sale unei sume ponderate de semnale este egal cu suma ponderată de rezultate obținute aplicând acea reprezentare fiecărui semnal. În continuare, sunt prezentate câteva dintre reprezentările timp-frecvență cele mai importante.

1.1.1. Transformarea Fourier scurtă (STFT)

Transformarea Fourier (FT) este binecunoscută ca fiind instrumentul matematic clasic de transformare din domeniul timp în domeniul frecvență. Pentru un semnal $s(t)$, transformarea FT este definită astfel:

$$S(f) = \int_{-\infty}^{+\infty} s(t) e^{-j2\pi ft} dt \quad (1.1)$$

Relația (1.1) ne arată că FT este de fapt produsul scalar dintre funcția $s(t)$ și o exponențială complexă, de frecvență f și durată infinită. Prin urmare, această reprezentare nu permite localizarea în timp, fiind total nepotrivită în analiza semnalelor netaționare.

Pentru a elimina inconvenientele transformării FT, putem considera semnalul netaționar ca fiind local staționar, pe durata unei ferestre de timp $w(t)$, de lungime fixă. Astfel, printr-o analiză Fourier succesivă, ponderată cu o fereastră temporală se obține o reprezentare localizată simultan în timp și frecvență, numită transformarea Fourier scurtă (STFT), definită în relația (1.2) [Cohen95].

$$STFT_s(t, f) = \int_{-\infty}^{+\infty} s(t) w^*(t - \tau) e^{-j2\pi f\tau} d\tau \quad (1.2)$$

Deoarece STFT are valori complexe, în practică se reprezintă spectograma, definită ca și pătratul modulului transformării STFT. Ea este o reprezentare a densității spectrale de putere.

Pentru o mai bună localizare în timp, este necesară utilizarea unei ferestre de timp de lungime mică. Pe de altă parte există un compromis, deoarece reducerea lungimii ferestrei de analiză are ca efect înrăutățirea localizării în frecvență. Acest fapt este descris de principiul de incertitudine a lui Heisenberg-Gabor [Cohen95].

$$\Delta_t \Delta_f \geq \frac{1}{4\pi} \quad (1.3)$$

unde Δ_t și Δ_f reprezintă rezoluția temporală și frecvențială.

În conformitate cu acest principiu, niciun semnal nu poate fi perfect localizat atât în domeniul timp, cât și în domeniul frecvență. Compromisul cel mai bun este

obținut folosind o fereastră de timp, de tip Gauss. Transformarea rezultată este cunoscută sub numele de transformarea Gabor (GT).

În figura 1.1 este reprezentat pavajul timp-frecvență în cazul STFT în comparație cu pavajul în cazul Shannon și Fourier.

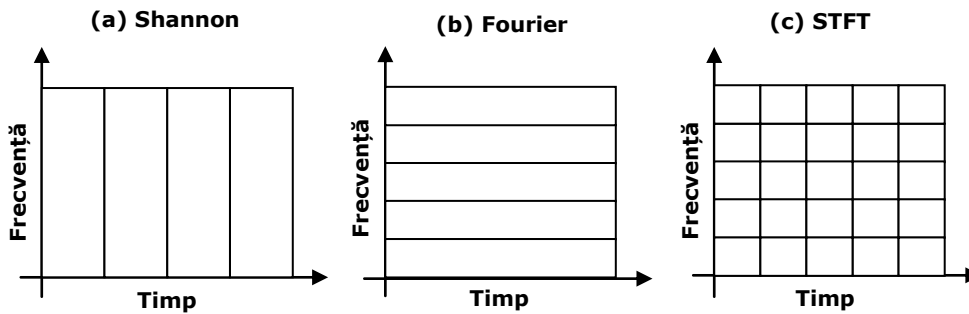


Figura 1.1. Pavajul timp-frecvență: Shannon (a) Fourier (b) și STFT (c)

1.1.2. Transformarea Wavelet (WT)

Un alt tip de reprezentare liniară care rezolvă rezoluția fixă a STFT, este transformarea Wavelet (WT). WT oferă o acoperire a planului timp-frecvență într-o manieră eficientă, prin utilizarea unor ferestre cu o lungime flexibilă, care se îngustează la frecvențe ridicate și se dilată la frecvențe scăzute. Prin urmare, se obține o rezoluție temporală bună la frecvențe înalte, și la o rezoluție în frecvență bună pentru frecvențele joase. Acest lucru este dezirabil pentru analiza semnalelor cel mai des întâlnite în practică, pentru care frecvențele joase au o evoluție lentă, de durată lungă, în timp ce frecvențele înalte se regăsesc în tranziții bruște și de scurtă durată.

Transformarea WT a unui semnal se obține prin descompunerea într-o familie de funcții translatate în timp și scalate, plecând de la o funcție unică $\psi(t)$, numită undișoara mamă ("wavelet mother"). Familia de undișoare este:

$$\psi_{\tau,a}(t) = \frac{1}{\sqrt{a}} \psi\left(\frac{t-\tau}{a}\right) \quad (1.4)$$

Prin urmare, transformarea WT pentru semnalul $s(t)$, se poate scrie:

$$WT_S(\tau, a) = \int_{-\infty}^{+\infty} s(t) \psi_{\tau,a}^*(t) dt \quad (1.5)$$

Folosind o asemenea reprezentare, planul timp-frecvență este partajat într-o manieră flexibilă. În figura 1.2 este ilustrată modalitatea în care "atomii" timp-frecvență sunt localizați cu ajutorul funcțiilor wavelet.

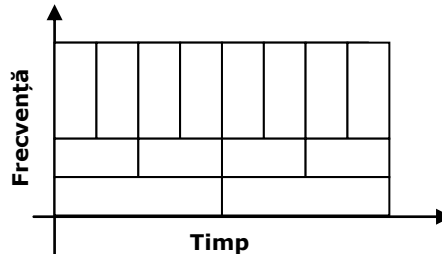


Figura 1.2. Partajarea planului timp-frecvență pentru WT

Transformarea WT indicată prin relația (1.5) constituie versiunea continuă a transformării wavelet. Aceasta prezintă o redundanță ridicată, ceea ce o face dificil de aplicat în multe situații practice. Cu scopul de a obține o reprezentare neredundantă și cu posibilitatea sintezei perfecte a semnalului, [Mal89] a propus un algoritm eficient și flexibil, cunoscut sub numele de analiză multirezoluție. Calculul versiunii discrete a transformării wavelet (DWT) este posibil grație algoritmului lui Mallat. Așadar, DWT analizează semnalul în diverse benzi de frecvență cu diverse rezoluții, prin descompunerea acestuia în informație (coeficienți) de aproximare, respectiv de detaliu. În acest scop, DWT utilizează două seturi de filtre, trece-jos (FTJ) și trece-sus (FTS). Răspunsurile la impuls ale acestor filtre sunt $g[n]$, respectiv $h[n]$. Descompunerea semnalului în diverse subbenzi este obținută prin aceste operații succesive de filtrare trece jos și trece sus. După filtrare, procedura de analiză presupune și o subeșantioane (decimare). Pe de altă parte, la fiecare iterație a transformării inverse folosite în reconstrucție, semnalul este supraeșantionat și trecut prin filtrele de sinteză $g'[n]$ și $h'[n]$. În figura 1.3 sunt reprezentate schematic operatorul de analiză, respectiv operatorul de sinteză.

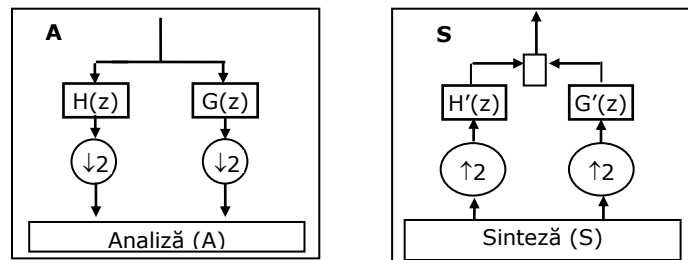


Figura 1.3. Operatorii de descompunere și de reconstrucție în analiza multirezoluție

1.2. RTF biliniare

1.2.1. Distribuția Wigner-Ville (WVD)

Distribuția Wigner-Ville (WVD) a fost introdusă în 1948 de către Ville, putând fi interpretată ca și o distribuție de energie [Cohen95]. Această transformare este definită ca fiind transformarea Fourier a funcției de autocorelație instantanee (denumită și momentul instantaneu de ordinul doi).

$$WVD_s(t, f) = \int_{-\infty}^{+\infty} s\left(t + \frac{T}{2}\right) s^*\left(t - \frac{T}{2}\right) e^{-j2\pi ft} dt \quad (1.6)$$

Distribuția WVD are o serie de proprietăți utile [Cohen95]: localizarea perfectă a structurilor timp-frecvență liniare, conservarea energiei, conservarea suportului temporal și frecvențial, etc. Cu toate acestea, WVD prezintă un inconvenient major: datorită biliniarității transformării apar termeni de interferență între diferitele componente ale semnalului. Dacă se consideră două semnale $x(t)$ și $y(t)$, atunci WVD a sumei celor două semnale este:

$$WVD(t, f) = WVD_x(t, f) + WVD_y(t, f) + 2\Re\{WVD_{xy}(t, f)\} \quad (1.7)$$

În figura 1.4 este pusă în evidență geometria în planul timp-frecvență, a acestor termeni de interferență. Analizând figura 1.4, se observă pe lângă termenii utili corespunzători celor două componente spectrale, și termeni de interferență cu o structură oscilantă. Existența acestor termeni de interferență poate afecta procesul de decizie.

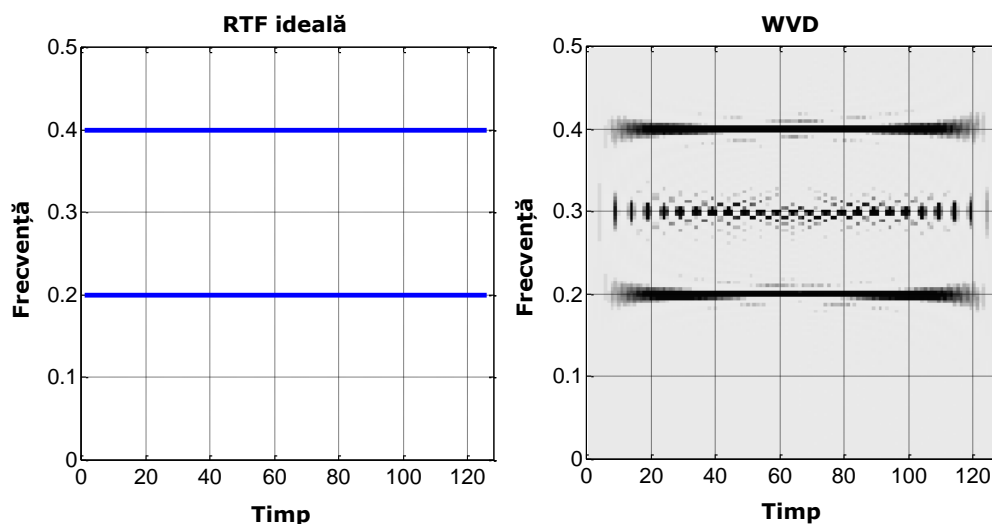


Figura 1.4. Termenii de interferență a WVD

1.3. RTF bazate pe modelarea polinomială a fazei semnalelor

1.3.1. Caracterizarea polinomială a fazei

Semnalele întâlnite în multe din aplicațiile tehnologice (sistemele RADAR și SONAR, sistemele de comunicații mobile, prelucrarea semnalelor submarine, biomedicale, etc.) au un comportament puternic neliniar, și implică de obicei o modulație de frecvență (FM) sau de amplitudine (AM). În practică, s-a constatat că

pentru majoritatea din aceste semnale, funcția de fază poate fi modelată printr-un polinom. Un semnal $s(t)$, cu fază polinomială (PPS) este definit prin relația:

$$s(t) = A \exp j^{\phi(t)} = A \exp \left[j \sum_{k=0}^K a_k t^k \right] \quad (1.8)$$

Acest model este unul parametric, faza semnalului $\phi(t)$ fiind caracterizată printr-un număr restrâns de coeficienți $\{a_k\}$. De exemplu, pentru un ordin de aproximare $K=1$, se obține un semnal sinusoidal, pentru $K=2$ un semnal chirp.

O abordare clasică pentru estimarea coeficienților polinomiali a fost introdusă în [Porat93], bazată pe funcția de ambiguitate de ordin superior (HAF). Această metodă presupune utilizarea unui moment instantaneu de ordinul 2, asemănător celui folosit în distribuția WVD:

$$M_2(t, \tau) = s(t)s^*(t - \tau) \quad (1.9)$$

Iterativ, momentul de ordinul K se poate obține calculând momentul instantaneu de ordinul 2 pentru momentul de ordin $K-1$:

$$M_K(t, \tau) = M_2[M_{K-1}(t, \tau)](t, \tau) \quad (1.10)$$

Momentul instantaneu de ordinul K are ca efect reducerea unui semnal PPS la o simplă componentă armonică de timp complexă:

$$M_K(t, \tau) = A^{2^{K-1}} \exp(K! \tau^{K-1} a_k t + \phi_k) \quad (1.11)$$

Având în vedere aceste proprietăți, procedura de estimare secvențială a coeficienților este ilustrată în figura 1.5. Algoritmul presupune cunoașterea inițială a ordinului polinomial K al fazei.

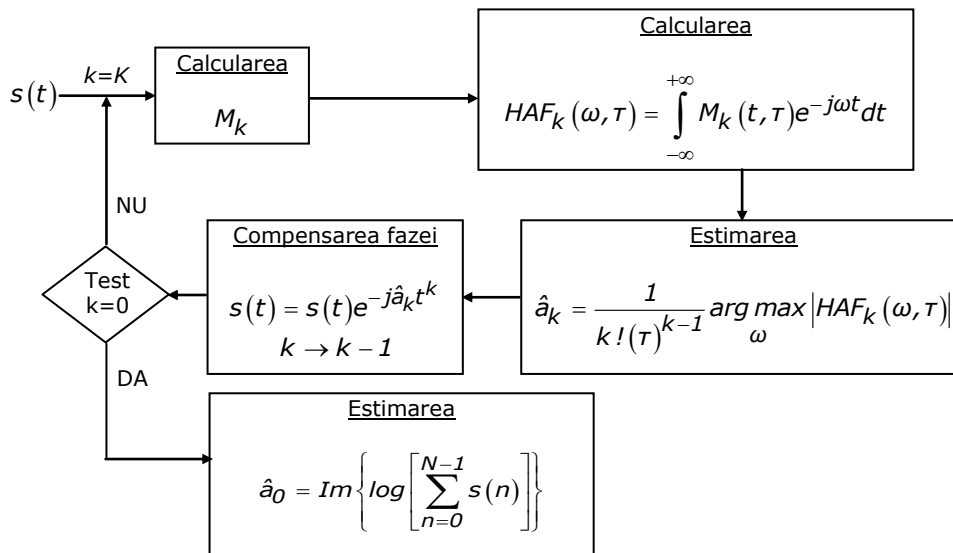


Figura 1.5. Algoritm de estimare a coeficienților polinomiali

Această metodă neliniară prezintă însă câteva dezavantaje majore legate de robustețea la zgomot, prezența termenilor de interferență pentru semnale PPS multi-componente precum și efectul de propagare a erorii în procesul de compensare a fazei.

Pentru eliminarea primelor două limitări, în [Barb96] se propune o generalizare a momentelor de ordin superior, prin utilizarea unui set distinct de întârzieri $\tau_i = (\tau_1, \dots, \tau_i)$:

$$M_K(t, \tau_{K-1}) = M_{K-1}(t + \tau_{K-1}, \tau_{K-2}) M_{K-1}^*(t - \tau_{K-1}, \tau_{K-2}) \quad (1.12)$$

Aplicând transformata Fourier, rezultă funcția de ambiguitate de ordin superior multi-întârziere (ml-HAF):

$$ml-HAF_K(\omega, \tau_{K-1}) = \int_{-\infty}^{+\infty} M_K(t, \tau_{K-1}) e^{-j\omega t} dt \quad (1.13)$$

Performanțele metodei ml-HAF pot fi semnificativ îmbunătățite, prin multiplicarea mai multor funcții HAF obținute pentru diferite seturi de întârzieri. Este vorba despre metoda ml-HAF multiplicativă (ml-PHAF) [Barb98].

1.3.2. Reducerea ordinului polinomial cu ajutorul tehnicii de deformare. Metoda ("WarpComp")

Sunt situații în care pentru anumite semnale PPS, este necesar un model polinomial de aproximare de ordin mai mare. În aceste cazuri, datorită efectului de propagare a erorii ce apare datorită mecanismului de compensare a fazei, din procesul de estimare recursiv, metodele prezentate în paragraful anterior sunt practic inutilizabile. Prin urmare, pentru reducerea propagării erorilor, este necesară introducerea unei metode alternative de reducere a ordinului polinomial. În [Ioana03] este prezentată o astfel de tehnică bazată, pe operatorii de deformare a semnalelor.

Metoda presupune construirea unei funcții de deformare temporală:

$$w_K : t \xrightarrow{w_K} t_w^{(K)} = w_K(t) = \left(\frac{t}{|\hat{a}_K|} \right)^{1/K} \quad (1.14)$$

unde \hat{a}_K este coeficientul estimat de ordinul K . Se aplică apoi operatorul de deformare, definit în relația următoare:

$$(U_K s)(t) = \sqrt{w_K'(t)} s(w_K(t)) \quad (1.15)$$

Efectul asociat transformării de mai sus, aplicate unui semnal PPS de ordinul K , pentru noua variabilă de timp $t_w^{(K)}$, este un semnal PPS de ordinul $K-1$. În plus, coeficientul de ordinul $K-1$ este dependent doar de coeficientul de ordin K , eliminându-se astfel propagarea erorii de estimare la ordinele polinomiale inferioare. Acest proces este repetat până la estimarea tuturor coeficienților polinomiali. Procedura de compensare a fazei este prezentată în figura 1.6.

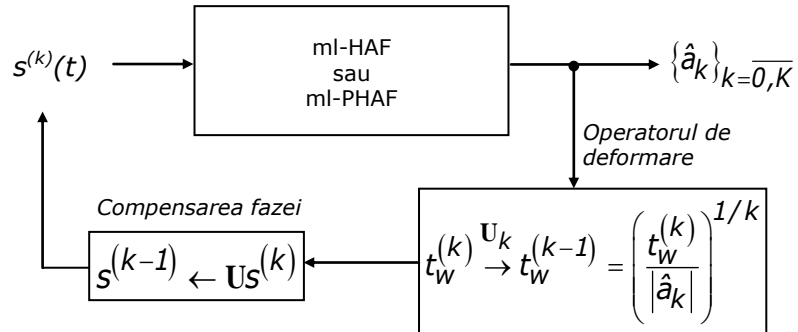


Figura 1.6. Reducerea ordinului polinomial bazată pe operatorul de deformare

Metoda de estimare a coeficienților polinomiali ce utilizează compensarea de fază mai sus prezentată, este denumită metoda "WarpComp".

2. APLICAȚII ALE RTF PENTRU SEMNALE CU FAZĂ POLINOMIALĂ

2.1. Recunoașterea modulațiilor multi-purtătoare bazată pe metoda WarpComp

2.1.1. O privire generală asupra semnalelor de comunicații

Recunoașterea tipului de modulație digitală a unui semnal a cunoscut, în ultimele decenii, o largă utilizare. Diverse semnale de comunicații se întâlnesc în majoritatea standardelor și aplicațiilor de transmisiuni pe canale radio sau cu fir. Se pot enumera aici standardele DAVB (Digital Audio and Video Broadcasting), IEEE 802.11 (rețele WiFi), IEEE 802.16 (WiMAX), modemurile de mare viteză, aplicațiile din domeniul militar (războiul electronic, supraveghere, etc.).

În funcție de numărul de purtătoare folosite, tehnicile de modulație se împart în două mari categorii: modulații mono-purtătoare, respectiv modulații multi-purtătoare. Din prima categorie fac parte: modulația FSK (Frequency Shift Keying), PSK (Phase Shift Keying), ASK (Amplitude Shift Keying). În a doua categorie de metode se încadrează: OFDM (Orthogonal Frequency Division Multiplexing), WOFDM (Wavelet-based OFDM).

Semnalul modulat în frecvență se obține prin modificarea frecvenței purtătoare și este descris de ecuația următoare:

$$s_{FSK}(t) = A_c \cos \left[\omega_c t + \Delta\omega \int_0^t x(\tau) d\tau + \theta \right] \quad (2.1)$$

Unde $\Delta\omega$ reprezintă variația maximă de frecvență ce apare în procesul de modulare. Frecvența variază în funcție de mesajul de informație $x(t)$, prin urmare informația utilă este conținută în frecvența instantanee. Avantajele modulației de frecvență sunt: rezistența la perturbații, putere de transmisie constantă, independența față de atenuarea canalului de comunicație. În schimb, are o eficiență scăzută în utilizarea benzii alocate, modulația FSK nefiind utilizată în sistemele de transmisiuni de mare viteză.

Modulația de fază presupune modificarea fazei unui semnal purtător pentru fiecare simbol de informație, cu o valoare ce depinde de secvența de biți ce trebuie transmisă. Această modulație este foarte robustă la perturbații, ocupă o bandă mai îngustă decât în cazul modulației FSK și necesită un factor de putere mai redus. Este utilizată în transmisiunile TV digitale prin satelit.

Semnalul PSK poate fi reprezentat prin:

$$s_{PSK}(t) = A_c \cos \left[\omega_c t + \sum_n \phi_n g(t - nT) \right] \quad (2.2)$$

în care $g(t-nT)$ este un impuls dreptunghiular unitar de durată T , iar $\{\phi_n\}$ o secvență de faze corespunzătoare simbolurilor emise.

Modulația de amplitudine este o modulație liniară utilizată la transmiterea semnalelor binare. Expresia matematică a semnalului ASK este dată de:

$$s_{ASK}(t) = \sum_n a_n g(t-nT) \cos(\omega_c t) \quad (2.3)$$

unde $\{a_n\}$ reprezintă secvența simbolurilor transmise, de durată T .

În comparație cu tipurile de modulații prezentate anterior, ideea de bază a modulației OFDM este transmisia simultană multi-purtătoare, pe mai multe subcanale de bandă relativ îngustă. În plus, purtătoarele folosite sunt ortogonale între ele. Toate acestea duc la creșterea eficienței spectrale și ameliorarea problemelor ridicate de către selectivitatea în frecvență a canalului.

Modelul matematic corespunzător transmisiei a M simboluri OFDM pe câte N subpurtătoare este descris de relația:

$$s_{OFDM}(t) = \sum_{l=0}^{M-1} \sum_{k=0}^{N-1} X_{l,k} e^{j2\pi f_k t} p(t-lT) e^{j2\pi f_c t} \quad (2.4)$$

unde $X_{l,k}$ reprezintă simbolul de informație cu indexul k aparținând blocului OFDM cu indexul l , f_c este frecvența semnalului purtător și $f_k = f_0 + k\Delta f$ este frecvența subpurtătoarei cu indexul k , iar $p(t)$ reprezintă funcția formatoare de impulsuri.

2.1.2. Principiul de identificare a modulațiilor numerice

Identificarea semnalelor de comunicații a devenit o disciplină independentă în războiul electronic. Scopul este de a intercepta, analiza, clasifica și înțelege semnalele de comunicații.

În [Sal04] am propus o metodă de identificare a modulației OFDM, bazată pe o tehnică de filtrare cu o baterie de filtre ortogonale și pe procedura de estimare "WarpComp" descrisă în paragraful 1.4.2. Planul timp-frecvență a unui semnal OFDM este unul complex, datorită numeroaselor purtătoare conținute în semnal. Meoda presupune recuperarea și localizarea frecvențelor purtătoare din banda de frecvență de interes a semnalului modulat, în scopul discriminării diferitelor tipuri de modulații numerice. În figura 2.1 se prezintă schema bloc generală de prelucrare, ce stă la baza metodei propuse.

2.1 – Recunoașterea modulațiilor multi-purtătoare bazată pe metoda WarpComp 17

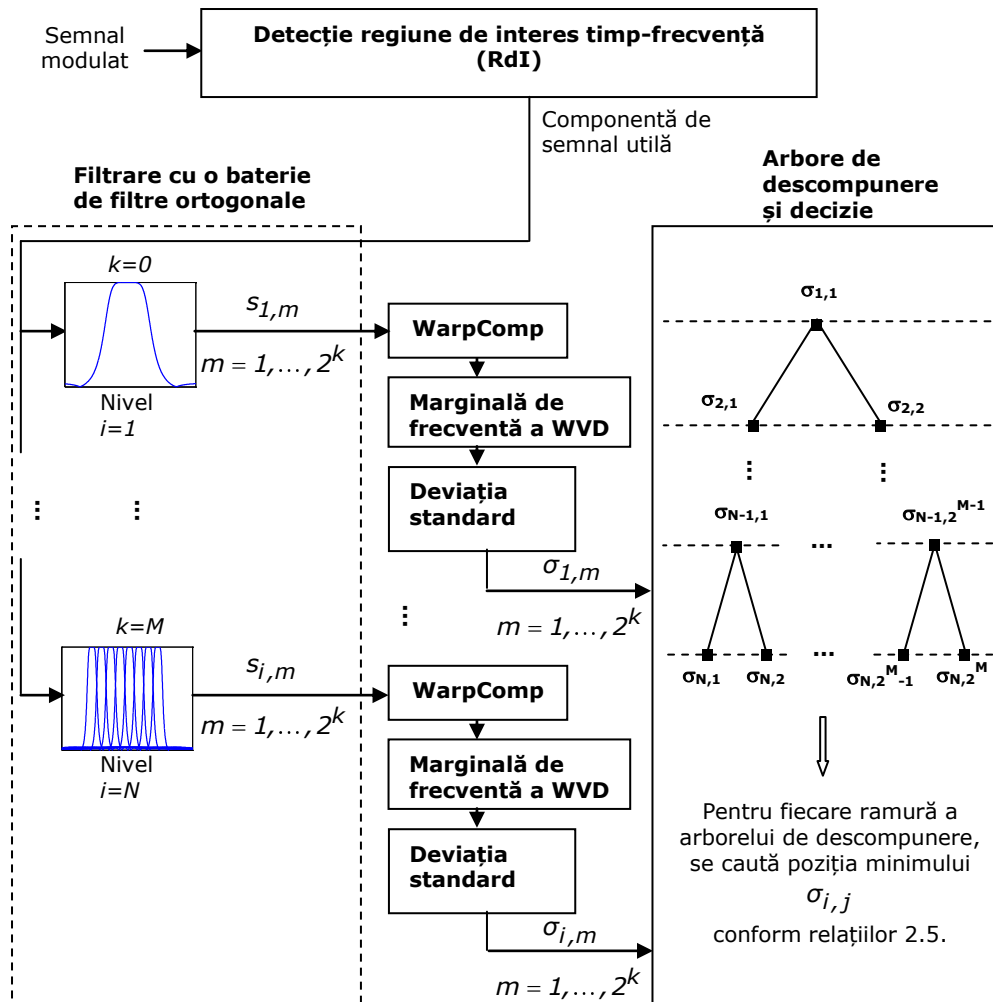


Figura 2.1. Schema bloc generală de prelucrare pentru identificarea modulației OFDM

Inițial, semnalul de intrare modulat este supus unei detecții a benzii de frecvență utile din spectrul total, în care se regăsesc frecvențele purtătoare. Detecția se bazează pe utilizarea mărimii statisticii de ordin superior de tipul cumulant de ordinul 4 [Cornu06]. Metoda timp-frecvență de identificare a tipurilor de modulații prezentată mai sus, se aplică ulterior doar în această regiune de interes (RdI) detectată din semnalul analizat. Urmează apoi o filtrare în sub-benzi, pe un număr de N niveluri. În fiecare din aceste niveluri de descompunere, se construiește o baterie de filtre ortogonale compusă din filtre, unde $k=1,2,\dots,N$. Semnalele de comunicații cu modulații mono-purtătoare și modulații multi-purtătoare prezentate anterior, au o caracteristică comună: expresia fazei poate fi modelată printr-un polinom. Prin urmare, momentele de ordin superior introduse în paragraful 1.4, și mai exact tehnica de estimare a coeficienților polinomiali "WarpComp", constituie o metodă adecvată prelucrării acestor tipuri de semnale. Astfel, semnalul filtrat

obținut la ieșirea fiecărui filtru, este adus la intrarea blocului "WarpComp" obținându-se semnalul staționarizat. În cazul OFDM, în urma filtrării cu elementele bateriei de filtre ortogonale de pe ultima linie, se separă fiecare purtătoare. Acestea sunt semnale cu faza inițială constantă. Deci corespund la polinoame de ordinul zero. În consecință tehnica "WarpComp" nu le modifică. În continuare, se calculează marginala de frecvență a WVD, determinându-se de asemenea și deviația standard $\sigma_{i,j}$, corespunzătoare distribuției normale rezultate pe baza marginalei de frecvență, unde i reprezintă nivelul de descompunere iar j poziția filtrului din bateria de filtre de pe nivelul respectiv. Un semnal bine staționarizat înseamnă o detecție corectă a unei frecvențe purtătoare din spectru, ceea ce duce la obținerea unei valori mici a deviației standard echivalente. Aceasta este proprietatea care stă la baza metodei propuse pentru identificarea modulațiilor numerice.

În ceea ce privește arborele de descompunere folosit, el este construit în maniera ilustrată în figura 2.1, de la primul nivel până la ultimul nivel de descompunere. Pentru fiecare ramură a arborelui se determină poziția minimumului $\sigma_{i,j}$, conform relațiilor (2.5).

$$\begin{aligned}
 \sigma^{(1)} &= \min\{\sigma_{N,1}, \sigma_{N-1,1}, \dots, \sigma_{2,1}, \sigma_{1,1}\} \\
 \sigma^{(2)} &= \min\{\sigma_{N,2}, \sigma_{N-1,1}, \dots, \sigma_{2,1}, \sigma_{1,1}\} \\
 &\dots \\
 \sigma^{(2^M-1)} &= \min\{\sigma_{N,2^M-1}, \sigma_{N-1,2^M-1}, \dots, \sigma_{2,2}, \sigma_{1,1}\} \\
 \sigma^{(2^M)} &= \min\{\sigma_{N,2^M}, \sigma_{N-1,2^M-1}, \dots, \sigma_{2,2}, \sigma_{1,1}\}
 \end{aligned} \tag{2.5}$$

Recunoașterea unei modulații mono-purtătoare sau a unei modulații multi-purtătoare este dată de repartizarea diferită a acestor minime în arborele de descompunere. Rezultatele obținute sunt prezentate în paragraful 2.1.3.

2.1.3. Rezultate

Primul semnal folosit pentru testare este reprezentat în figura 2.2. Este un semnal de tip OFDM multi-purtătoare obținut prin însumarea a patru semnale QPSK (Quadrature Phase Shift Keying) cvasi-analitice, având următoarele frecvențe purtătoare normalizate: 0.200, 0.224, 0.248 și 0.273. Lungimea semnalului este de 1024 eșantioane.

2.1 – Recunoașterea modulațiilor multi-purtătoare bazată pe metoda WarpComp 19

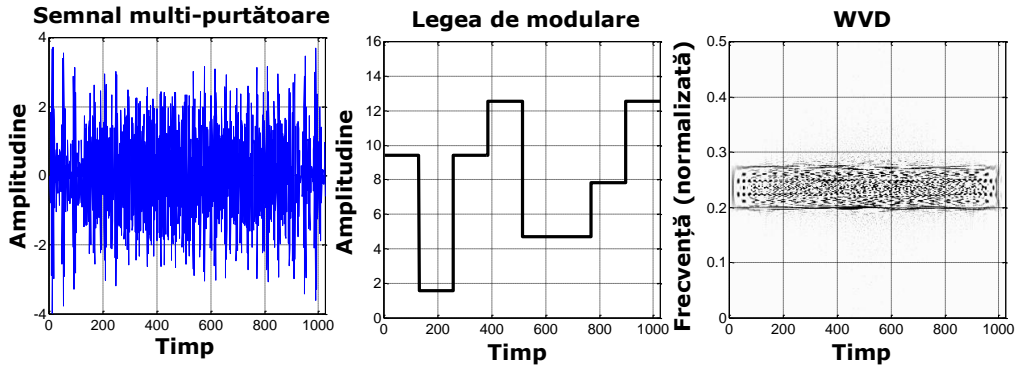


Figura 2.2. Exemplu de modulație multi-purtătoare

Analizând reprezentarea WVD din figura 2.2, se observă complexitatea spectrală a semnalului multi-purtătoare datorată celor patru purtătoare folosite în procesul de modulație. Banda de frecvență rezultată în urma etapei de detecție a regiunii de interes timp-frecvență este $[0.179, 0.295]$. Numărul de niveluri de descompunere este $N=3$, bateria de filtre ortogonale având pe fiecare nivel: 1 filtru, 2 filtre respectiv 4 filtre. Filtrele utilizate sunt de tipul Cebășev II. La generarea bateriilor de filtre s-a avut în vedere informația privind numărul de purtătoare din semnal, precum și spațierea lor spectrală. Bateriile de filtre sunt prezentate în figura 2.3. În aceeași figură este ilustrată și localizarea în frecvență a purtătoarelor. Pentru metoda "WarpComp" ordinul de aproximare polinomial considerat este $K=10$.

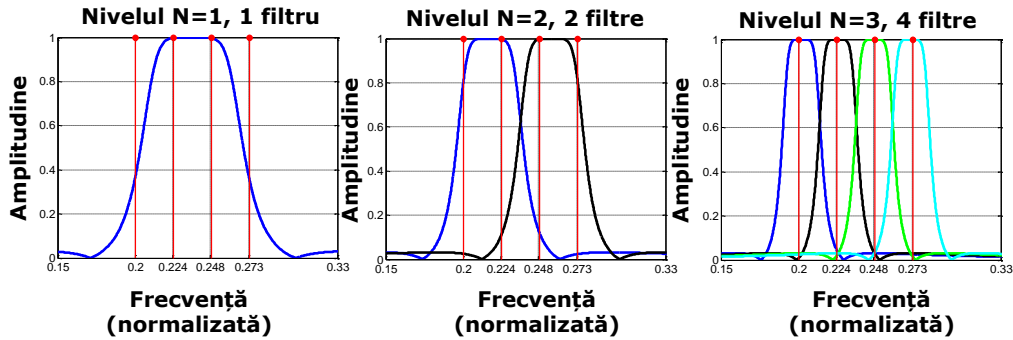


Figura 2.3. Caracteristica de frecvență a filtrelor de tip Cebășev II, pentru $N=3$ niveluri de descompunere

În urma simulărilor, a rezultat că valorile minime pentru cele 4 ramuri ale arborelui de descompunere sunt localizate în totalitate pe nivelul 3, frecvențele purtătoare fiind perfect identificate. Într-adevăr, analizând figura 2.3, se poate observa că bateria cu 4 filtre are cea mai bună poziționare spectrală în raport cu frecvențele purtătoare.

Următorul semnal analizat este un semnal QPSK cvasi-analitic cu frecvența purtătoare normalizată 0.248, redat în figura 2.4. Parametrii de simulare sunt aceiași ca și în cazul semnalului multi-purtătoare analizat anterior.

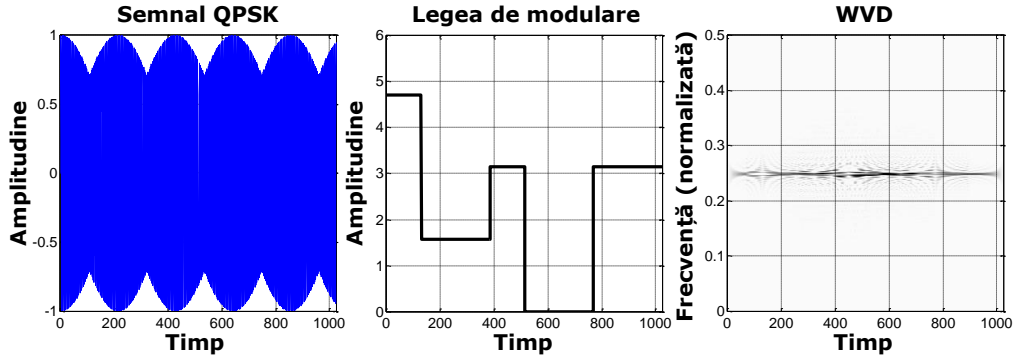


Figura 2.4. Exemplu de modulație QPSK

În acest caz, rezultatele obținute arată o repartizare diferită a valorilor minime ale deviației standard în arborele de descompunere: un minim pe nivelul 1 în poziția (1,1) și un singur minim pe nivelul 3 în poziția (3,3). În comparație cu cazul multi-purtătoare, în care minimele sunt distribuite majoritar pe nivelul inferior $N=3$, în cazul QPSK minimele sunt regăsite în număr mai redus, pe nivelul superior $N=1$ și pe nivelul inferior $N=3$. Din aceste rezultate, pe baza dispunerii diferite a valorilor minime pe fiecare ramură a arborelui de descompunere, este posibilă separarea modulației multi-purtătoare de celelalte modulații mono-purtătoare.

Pentru evaluarea performanțelor schemei propuse în figura 2.1, s-au considerat 100 de semnale cu 4 purtătoare și 100 de semnale cu modulație QPSK. Rezultatele sunt prezentate în tabelele 2.1 și 2.2.

Număr purtătoare	1	2	3	4
Nivel 1	0	0	0	0
Nivel 2	0	0	0	0
Nivel 3	0	2	28	70

Tabel 2.1. Performanțele privind numărul de purtătoare detectate, $N=3$ niveluri și 100 semnale multi-purtătoare

Număr purtătoare	1	2	3	4
Nivel 1	100	0	0	0
Nivel 2	0	0	0	0
Nivel 3	74	16	0	0

Tabel 2.2. Performanțele privind numărul de purtătoare detectate, $N=3$ niveluri și 100 semnale QPSK

Din tabelul 2.1 se observă performanță bună de detecție a purtătoarelor, în 70 de realizări fiind detectate toate cele 4 purtătoare pe ultimul nivel, în 28 de realizări doar 3 din ele și doar în 2 realizări numai 2 purtătoare. În schimb, tabelul

2.1 – Recunoașterea modulațiilor multi-purtătoare bazată pe metoda WarpComp 21

2.2 arată un tipar de comportament diferit în ceea ce privește numărul de purtătoare detectate: o singură purtătoare s-a detectat pe primul nivel în toate cele o sută de realizări iar în 74 de realizări pe ultimul nivel de descompunere. În 16 realizări s-au obținut 2 purtătoare.

În continuare, sunt prezentate rezultatele simulării utilizând două semnale de comunicații, din baza de date [COMINT04]. Parametrii acestor semnale precum și a bateriilor de filtre sunt ilustrați în tabelul 2.3. Modelul polinomial considerat este $K=10$.

PARAMETRII			
Semnalul multi-purtătoare		Semnalul FSK	
Frecvența de eșantionare	250 kHz	Frecvența de eșantionare	250 kHz
Număr de purtătoare	32	Număr de purtătoare	1, localizată la 25 kHz
Raportul semnal pe zgomot	$SNR=5dB$	Raportul semnal pe zgomot	$SNR=0dB$
Număr de eșantioane	3201	Număr de eșantioane	2000
Număr de simboluri	9	Număr de simboluri	200
Bateria de filtre		Bateria de filtre	
Banda de frecvență de interes	[10, 41] kHz	Banda de frecvență de interes	[2.9, 47.1] kHz
Niveluri de descompunere	6	Niveluri de descompunere	6
Tip filtre	Cebâșev II	Tip filtre	Cebâșev II

Tabel 2.3. Parametrii semnalelor de test din baza de date COMINT și a bateriilor de filtre utilizate

Vizual, distribuția rezultată a deviațiilor standard minime pe fiecare ramură a arborelui de descompunere este redată în figura 2.5 pentru semnalul cu modulație multi-purtătoare și în figura 2.6 pentru semnalul cu modulație FSK. Minimele sunt marcate în figură cu steluțe încercuite.

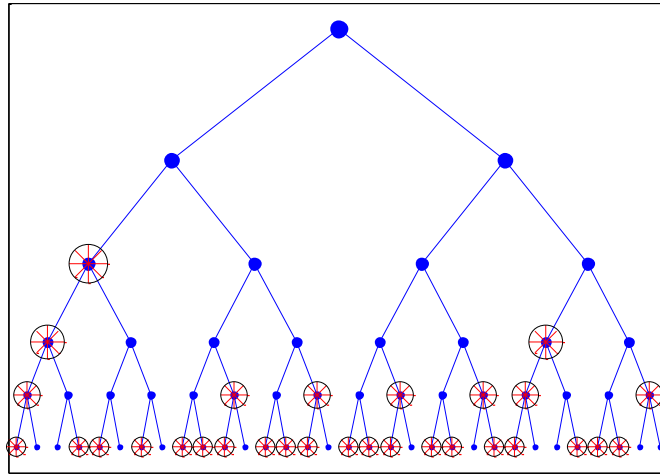


Figura 2.5. Arborele de descompunere rezultat pentru un semnal multi-purtătoare din baza de date COMINT

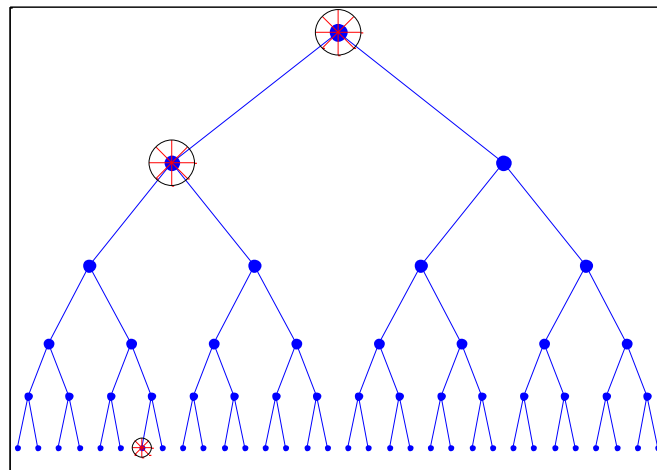


Figura 2.6. Arborele de descompunere rezultat pentru semnalul FSK din baza de date COMINT

Din analiza figurilor 2.5 și 2.6 se observă încă o dată structura diferită a arborilor de descompunere pentru semnalele considerate. În cazul multi-purtătoare avem un număr considerabil de minime, repartizate preponderent pe ultimele două niveluri, un lucru normal, întrucât bateriile de filtre de pe nivelul 5 și 6 sunt mai bine centrate pe cele 32 de frecvențe purtătoare. În schimb, în cazul FSK algoritmul propus a generat un număr mult mai mic de minime, datorate singurei purtătoare din semnal. În plus, putem remarca eficacitatea detecției purtătoarelor și pentru valori scăzute ale raportului semnal pe zgomot, chiar de 0dB.

În urma rezultatelor obținute și prezentate în acest paragraf, putem afirma că metoda propusă constituie o soluție foarte bună pentru recunoașterea modulațiilor mono și multi-purtătoare.

3. ESTIMAREA FRECVENȚEI INSTANTANEE BAZATĂ PE TEHNICI DE PRELUCRARE A IMAGINII

3.1. Considerații privind împrăștierea zgomotului în planul timp-frecvență

În prelucrarea semnalelor nestaționare, utilizarea RTF constituie deja o soluție consacrată, datorată în principal celor două caracteristici importante: concentrarea foarte bună în jurul frecvenței instantanee (IF) și capacitatea de împrăștiere a zgomotului. Pentru analiza semnalelor perturbate de zgomot este folosită o reprezentare timp-frecvență care împrăștie componenta de zgomot în planul timp-frecvență. Această împrăștiere este cu atât mai bună cu cât reprezentarea timp-frecvență corespunzătoare corelează mai puțin zgomotul. Pe de altă parte, corelarea zgomotului are ca efect concentrarea puterii zgomotului în regiunile din planul timp-frecvență unde sunt localizate vârfurile TFR, problema estimării IF fiind în acest caz mult mai dificilă. În plus, dacă zgomotul este unul alb, împrăștierea este mai bună. În continuare se va prezenta efectul de împrăștiere a componentei de zgomot din semnal în cazul reprezentărilor timp-frecvență liniare și biliniare [Isar03].

Cazul RTF liniare

Fie un zgomot staționar $n(t)$. În general, expresia reprezentării timp-frecvență (TFR) pentru acest semnal este dată de relația:

$$TFR_n(t, \omega) = \int_{-\infty}^{\infty} n(\tau) \cdot K^*(\tau - t, \omega) d\tau \quad (3.1)$$

În funcție de expresia nucleului $K(\tau - t, \omega)$ se obțin expresiile unor RTF liniare diferite. Media statistică a mărimii din relația anterioară este:

$$E\{TFR_n(t, \omega)\} = M_n \cdot \int_{-\infty}^{\infty} K^*(\tau - t, \omega) d\tau \quad (3.2)$$

unde M_n reprezintă media zgomotului. De asemenea, funcția de corelație a TFR este dată de:

$$E\{TFR_n(t_1, \omega_1) TFR_n(t_2, \omega_2)\} = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} K^*(\tau_1 - t_1, \omega_1) \cdot K^*(\tau_2 - t_2, \omega_2) \cdot R_n(\tau_1 - \tau_2) d\tau_1 d\tau_2 \quad (3.3)$$

În relația (3.3) operatorul de corelație este notat cu R_n . Astfel, pentru un zgomot alb de medie nulă și deviație standard σ , corelația devine:

$$E \{ TFR_n(t_1, \omega_1) TFR_n(t_2, \omega_2) \} = \sigma^2 \cdot \int_{-\infty}^{\infty} K^*(\tau_1 - t_1, \omega_1) \cdot K^*(\tau_1 - t_2, \omega_2) d\tau_1 \quad (3.4)$$

Prin urmare, se observă că în cazul RTF liniare are loc corelarea zgomotului de intrare. Cu toate acestea, unele TFR liniare discrete nu prezintă această proprietate de corelație, un exemplu binecunoscut în acest sens fiind efectul de "albire" al transformării DWT. Totuși, TRF liniare realizează o împrăștiere a zgomotului în planul timp-frecvență, deoarece puterea semnalului la ieșirea sistemului ce implementează transformarea TFR din relația (3.1) este mai mică decât puterea semnalului de intrare $n(t)$. Într-adevăr, dacă se notează cu $n_o(t)$ acest semnal de ieșire, expresia puterii este [Isar03]:

$$\begin{aligned} E_{n_o} &= \frac{1}{2\pi} \cdot \int_{-\infty}^{\infty} |N_o(\omega)|^2 d\omega = \frac{1}{2\pi} \cdot \int_{-\infty}^{\infty} |N(\omega)|^2 \left| \mathfrak{F} \{ K^*(-t, \omega) \}(\omega) \right|^2 d\omega \leq \\ &\leq \frac{1}{2\pi} \cdot \int_{-\infty}^{\infty} |N(\omega)|^2 d\omega \cdot \int_{-\infty}^{\infty} \left| \mathfrak{F} \{ K^*(-t, \omega) \}(\omega) \right|^2 d\omega = \frac{1}{2\pi} \cdot \int_{-\infty}^{\infty} |N(\omega)|^2 d\omega = E_n \end{aligned} \quad (3.5)$$

Cazul RTF biliniare

TFR biliniară din clasa lui Cohen pentru semnalul $n(t)$, se poate calcula utilizând relația (3.6).

$$TF_n^C(t, \omega) = \frac{1}{2\pi} \cdot \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} n\left(s + \frac{\tau}{2}\right) \cdot n^*\left(s - \frac{\tau}{2}\right) \cdot e^{-j(\omega\tau - us + ut)} \cdot f(u, \tau) du ds d\tau \quad (3.6)$$

Media în acest caz este:

$$E \{ TFR_n(t, \omega) \} = \frac{1}{2\pi} \cdot \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} R_n(\tau) \cdot e^{-j(\omega\tau - us + ut)} \cdot f(u, \tau) du ds d\tau \quad (3.7)$$

Pentru un zgomot $n(t)$ alb de medie nulă și cu deviația standard σ , relația de mai sus se poate scrie:

$$E \{ TFR_n(t, \omega) \} = \sigma^2 \cdot f(0, 0) \quad (3.8)$$

De asemenea, corelația este:

$$\begin{aligned} E \{ TFR_n(t_1, \omega_1) TFR_n(t_2, \omega_2) \} &= \\ &= -\frac{\sigma^4}{2\pi} \cdot \mathfrak{F}_2 \{ f(u_2, \tau_1) \cdot f(-u_2, \tau_1) \}(\omega_1 + \omega_2, t_1 + t_2) + \sigma^4 \cdot f(0, 0) + \\ &+ \frac{\sigma^4}{\pi} \cdot \mathfrak{F}_2 \{ f(u_2, \tau_2) f(-u_2, \tau_2) \}(\omega_2 - \omega_1, t_2 - t_1) \end{aligned} \quad (3.9)$$

unde \mathfrak{F}_2 reprezintă transformarea Fourier bidimensională.

Din această clasă a lui Cohen, un caz aparte în acest context îl reprezintă distribuția WVD, care este de fapt o RTF de tipul densitate spectro-temporală de energie. Aplicând corelația din relația (3.9) se obține:

$$E \left\{ WVD_n(t_1, \omega_1) WVD_n(t_2, \omega_2) \right\} = 4\pi\sigma^4 \delta(\omega_2 - \omega_1) \delta(t_2 - t_1) + \sigma^4 - 2\pi\sigma^4 \delta(\omega_2 + \omega_1) \delta(t_2 + t_1) \quad (3.10)$$

Corelația în cazul WVD este un proces aleator bidimensional, asemănător unui zgomot alb bidimensional. Prin urmare, TFR din clasa lui Cohen corelează zgomotul de intrare, excepție făcând distribuția WVD, caz în care se realizează cea mai mare împrăștiere a zgomotului în planul timp-frecvență.

3.2. Rolul operatorilor morfologici

Morfologia matematică cuprinde o serie de operatori morfologici folosiți pentru descrierea formelor, fiind foarte potrivită în prelucrarea imaginilor. În general, interpretarea unei imagini presupune o etapă de segmentare (detecția și extragerea structurilor utile din imagine) și o etapă de cuantificare (clasificarea obiectelor identificate). Elaborată de matematicianul francez G. Matheron, morfologia matematică are la bază teoria mulțimilor, topologia, analiza funcțională și teoria probabilităților. El a introdus câțiva operatori morfologici de bază: erodarea, dilatarea, scheletizarea, etc. În esență, operatorii morfologici modifică forma obiectelor din imagine.

Fiecare imagine poate fi privită ca și o funcție f , definită pe o submulțime X a lui R^2 (suportul imaginii), cu valori în mulțimea Y . De exemplu, în cazul imaginilor binare, această funcție asociază fiecărui element al imaginii o valoare din mulțimea $\{0, 1\}$. Dacă se consideră însă funcția f_1 , restricția la mulțimea X_1 formată din elementele din imagine unde valoarea lui f este egală, să spunem cu 1, prin aplicarea unui operator morfologic acestei noi funcții, se obține funcția f_2 , care va descrie o mulțime de obiecte diferită. Se poate deci afirma că prin aplicarea operatorului morfologic considerat, forma obiectelor descrise de f_1 este modificată.

Operatorul de dilatare aplicat imaginilor binare (Anexa 1) are ca efect extinderea formelor din imagine prin utilizarea unor elemente structurante. Dilatarea morfologică are o serie de proprietăți: invarianță la translație, crescătoare, comutativă, asociativă și distributivă. Un exemplu de dilatare morfologică este ilustrată în figura 3.1. Imaginea inițială reprezintă distribuția WVD obținută pentru un semnal cu modulație parabolică de frecvență. Analizând figura, se pot desprinde câteva observații privind efectele operației de dilatare: obiectele din figură foarte apropiate sunt conectate, găurile mici sunt umplute, în timp ce obiectele care au dimensiunea egală cu dimensiunea elementului structurant utilizat sunt lărgite. Prin urmare, obiectele din imagine devin mai "îngroșate". Imaginea de eroare din figura 3.1 constituie diferența între imaginea obținută după dilatare și imaginea originală.

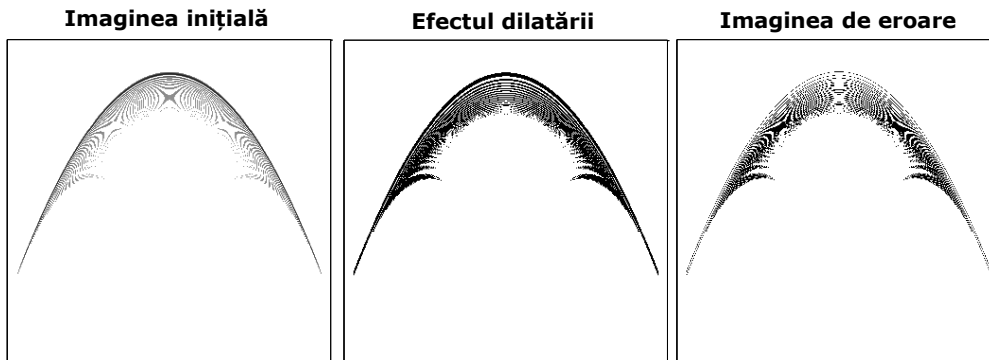


Figura 3.1. Efectul operatorului de dilatare asupra imaginilor

Îmbunătățirea informației vizuale în vederea optimizării analizei și interpretării, cunoaște diverse aplicații în domenii cum ar fi: medicină (prelucrarea imaginilor biomedicale), ecologie (studiul poluării utilizând imagini aeriene), criminalistică, apărare, industrie, etc.

Segmentarea este o etapă foarte importantă în procesul de prelucrare al imaginilor. Aceasta semnifică partajarea imaginii în zone omogene după anumite criterii de decizie, cu scopul de a recunoaște obiectele ce compun imaginea. Între operatorii de segmentare, scheletul morfologic ocupă o poziție privilegiată. Operatorul de scheletizare (Anexa 1) este o transformare morfologică mai complexă, compusă din mai multe operații morfologice de bază. Scheletul unui obiect, uneori numit și axa mediană a obiectului, poate fi definit în multe moduri. Aplicându-se diferite definiții se poate ajunge uneori la rezultate diferite. În figura următoare se prezintă efectul scheletizării unei imagini. Imaginea pentru care se calculează scheletul în acest caz, reprezintă a doua imagine din figura 3.1, imagine obținută în urma dilatării morfologice.

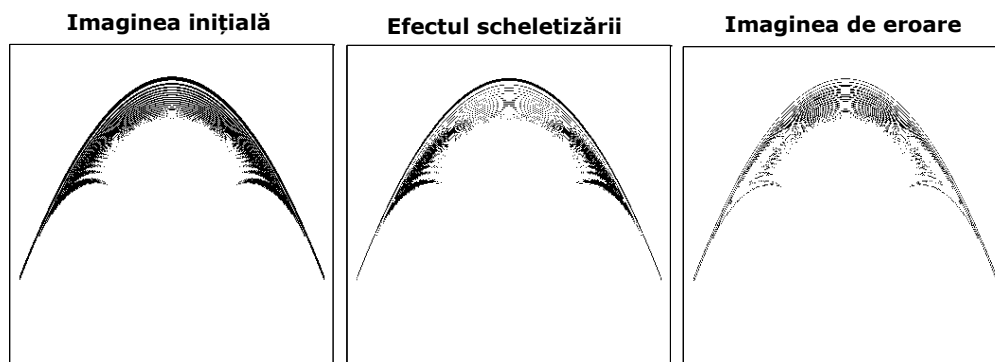


Figura 3.2. Efectul operatorului de scheletizare asupra imaginilor

Extragerea informațiilor dintr-o imagine este utilă în numeroase aplicații: analiza cu ajutorul calculatorului a informațiilor video, recunoașterea caracterelor, a formulelor chimice sau matematice, verificarea calității produselor, recunoașterea

prețurilor (coduri de bare), recunoașterea amprentelor și a feței, sortarea corespondenței, în meteorologie, apărare, etc.

3.3. Metoda RTF ce utilizează operatori morfologici în estimarea IF (TFR-MO)

În [BNI05] autorii au propus o metodă originală de estimare a frecvenței instantanee a unui semnal. Această metodă presupune calcularea unei reprezentări timp-frecvență obținută prin combinarea a două RTF clasice și utilizarea unui mecanism ingenios de extragere a vârfurilor din imaginea echivalentă (reprezentând curba IF din planul timp-frecvență), bazată pe operatori morfologici de prelucrare a imaginilor (TFR-MO). În figura 3.3 este ilustrată metoda TRF-MO.

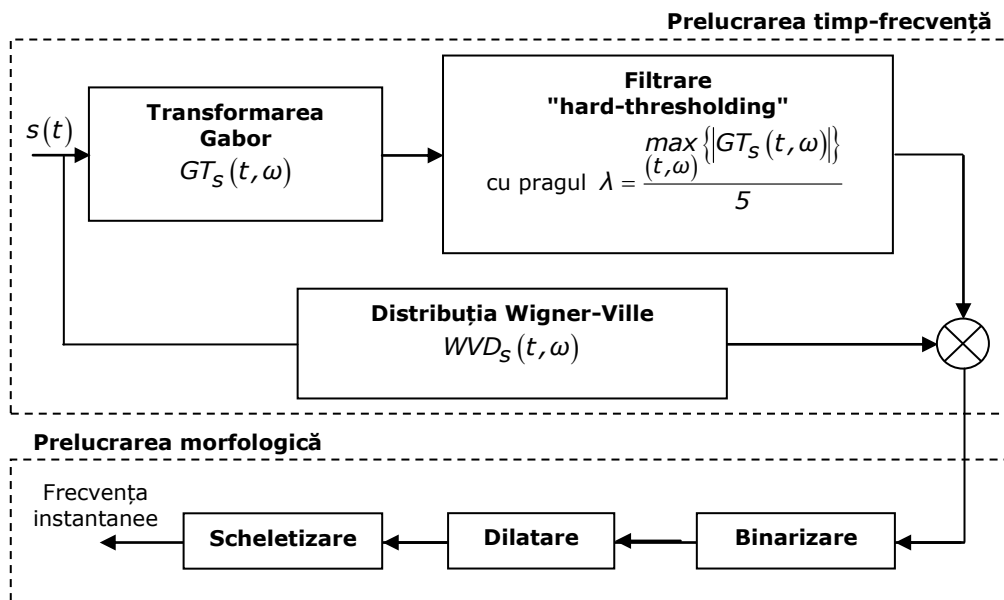


Figura 3.3. Metoda timp-frecvență de estimare IF bazată pe operatori morfologici (TFR-MO)

Din figură se observă că întregul proces de prelucrare cuprinde două etape: obținerea imaginii RTF și estimarea IF prin intermediul operatorilor morfologici. TFR propusă are în vedere avantajele oferite de către transformarea GT (localizare bună și absența termenilor de interferență) și de către distribuția WVD (localizare bună și efectul de împrăștiere a zgomotului). Prin calcularea GT puterea zgomotului prezent în semnalul de intrare este dispersată în întregul plan timp-frecvență, doar o mică parte a puterii zgomotului afectează zonele unde sunt localizate vârfurile RTF. În continuare, asupra GT se efectuează o filtrare de tip "hard-thresholding" cu un prag λ . Valoarea pragului utilizată este:

$$\lambda = \frac{\max\{|GT_S(t, \omega)|\}}{5} \quad (3.11)$$

Prin această operație de filtrare se urmărește reducerea zgomotului care perturbă vârfurile RTF și eliminarea lui în restul planului timp-frecvență.

Distribuția biliniară WVD, pe lângă localizarea foarte bună introduce și termeni de interferență care pot afecta estimarea corectă a curbei IF. Însă, prin multiplicarea distribuției WVD cu transformarea filtrată GT, termenii de interferență din planul timp-frecvență sunt îndepărtați în mare măsură, noua RTF obținută fiind astfel mult mai bine adaptată.

Algoritmul de estimare a vârfurilor RTF obținute anterior se bazează pe o prelucrare morfologică. Această etapă presupune aplicarea următorilor operatori morfologici:

- **Binarizarea** – realizează conversia imaginii în formă binară (fiecare pixel de imagine are doar două valori posibile: "1" pentru alb și "0" pentru negru). În plus, această operație are ca efect filtrarea imaginii, fiind echivalentă cu o procedură de eliminare a zgomotului.
- **Dilatarea** – datorită efectului de extindere, rolul operatorului de dilatare este de a compensa pierderea conectivității obiectelor din imagine (în acest caz, curba IF) datorată operațiilor de filtrare anterioare.
- **Scheletizarea** – prin aplicarea scheletului se obține estimarea IF a semnalului.

3.4. Studiul performanțelor TFR-MO

Semnalele de test utilizate în [BNI05] pentru evaluarea performanțelor metodei TRF-MO propuse, au fost semnale a căror frecvență instantanee nu avea o caracteristică foarte neliniară. Rezultatele obținute arată performanțe foarte bune chiar și pentru valori scăzute ale SNR. În paragrafele ce urmează, am analizat performanțele în estimarea IF a metodei TRF-MO pentru semnale mono-componente [Sal07] și multi-componente [Sala07], cu frecvența instantanee având tranziții rapide, adică un caracter puternic neliniar. De asemenea, este făcută și o analiză statistică.

3.4.1. Semnale mono-componentă

În continuare sunt prezentate rezultatele simulării care au fost făcute pentru estimarea IF folosind metoda TFR-MO pentru semnale mono-componente a căror frecvență instantanee este extrem de neliniară. În plus, am efectuat și un studiu comparativ al performanțelor de estimare al IF pentru diferite RTF.

Exemplul 1

Primul semnal de test considerat este un semnal cu fază polinomială și amplitudine constantă, $s(t)$, înecat de un zgomot gaussian alb, de medie nulă, $n(t)$. Semnalul are expresia:

$$s(t) = \exp\{j(5\pi t^3 - 9.5\pi t)\} + n(t) \quad (3.12)$$

Secvența alcătuită din 128 de eșantioane, cu t având valori în intervalul $[-1, 1]$, pentru un raport semnal pe zgomot SNR=3dB, este reprezentată în figura 3.4.

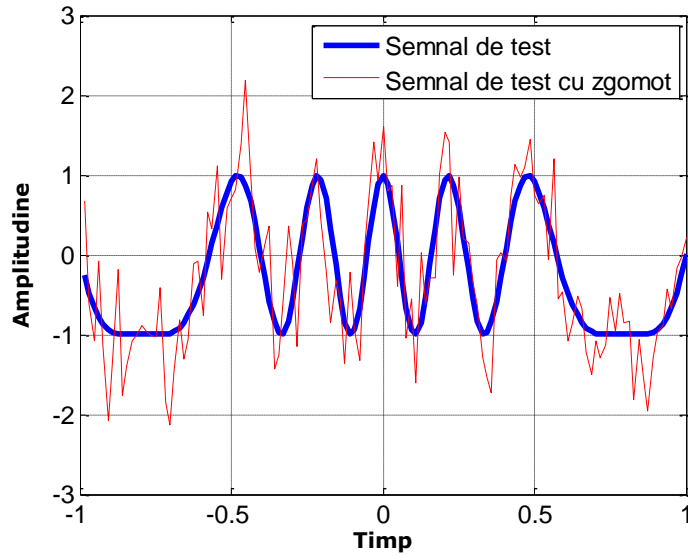


Figura 3.4. Semnal SFP cu amplitudine constantă, cu zgomot gaussian, SNR=3dB, exemplul 1

În figura 3.5 este prezentată estimarea IF utilizând metoda TRF-MO, pentru două valori diferite ale raportului semnal pe zgomot (SNR=3dB și SNR=30dB). Se observă din figură, că estimarea frecvenței instantanee este destul de bună pentru niveluri ridicate de zgomot.

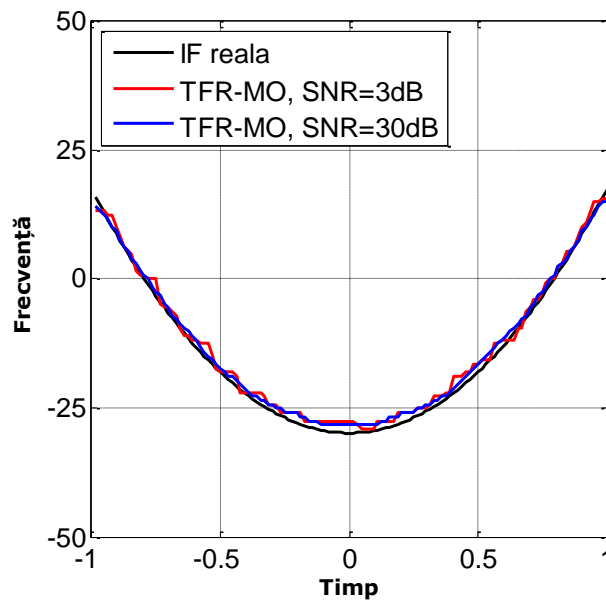


Figura 3.5. Estimarea IF prin metoda TFR-MO, exemplul 1

Pentru a pune în evidență performanțele metodei TFR-MO, în raport cu alte RTF clasice (WVD) și în raport cu distribuția de timp complexă (CTD) [Stank02], vom utiliza semnalul din figura 3.4. Rezultatele obținute pentru un raport semnal pe zgomot SNR=3dB și SNR=30dB sunt ilustrate în figura 3.6.

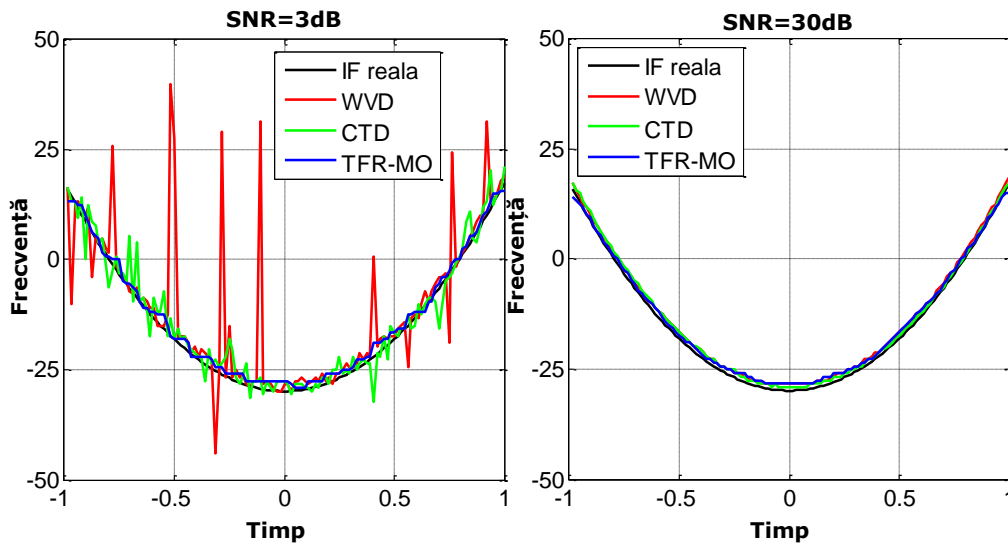


Figura 3.6. Comparație între TRF-MO și câteva reprezentări timp-frecvență, exemplul 1

Se observă că pentru un nivel scăzut de zgomot, abaterea și variația în jurul frecvenței instantanee estimate este foarte mică, rezultatele estimării IF fiind similare pentru toate cele trei metode analizate. În schimb, pentru valori mici ale SNR, estimarea IF prin WVD și CTD este puternic afectată de zgomot. Variația cea mai ridicată se obține pentru WVD, în timp ce CTD prezintă o variație mai mică. În aceste cazuri se constată o creștere foarte mare a variației odată cu creșterea zgomotului. Comparativ, rezultate mult mai bune se obțin însă pentru metoda TFR-MO, caz în care se observă o creștere moderată a varianței IF. Prin urmare metoda TFR-MO este mai robustă la zgomot.

Pentru o evaluare mai exactă a performanțelor estimării IF cu metodele vizate, în tabelul 3.1 sunt prezentate erorile medii pătratice de estimare (MSE) pentru diferite rapoarte semnal pe zgomot. Câteva observații se desprind din analiza acestor rezultate. În primul rând, se vede că nu există diferențe notabile în ceea ce privește performanța celor trei metode comparate, pentru cazurile SNR=30dB și SNR=15dB. Totuși, valorile cele mai mici ale erorii MSE, se obțin pentru TFR-MO. Diferențele sunt însă remarcabile pentru SNR=3dB, unde metodele CTD și WVD conduc la obținerea unor valori foarte mari ale erorii MSE (18.7804 respectiv 214.9682), comparativ cu valoarea MSE pentru TRF-MO (2.5856).

Ca o remarcă generală se poate observa că, așa cum era de așteptat, estimarea cea mai bună este obținută utilizând metoda TFR-MO, pentru toate cazurile luate în considerare.

RTF	SNR [dB]	MSE
TFR-MO	3	2.5856
	15	1.3348
	30	1.0189
CTD	3	18.7804
	15	1.6445
	30	1.3573
WVD	3	214.9682
	15	1.6675
	30	1.7247

Tabel 3.1. MSE al IF estimate, exemplul 1

În continuare se efectuează o analiză statistică a celor trei metode analizate și se compară performanțele lor. Analiză statistică a fost făcută pe 100 de realizări zgomotoase ale semnalului de test pentru un raport semnal pe zgomot cuprins între valorile 3 și 30dB cu un pas de 1dB. Valorile medii al erorilor MSE în funcție de raport semnal pe zgomot, SNR, sunt reprezentate în figura 3.7.

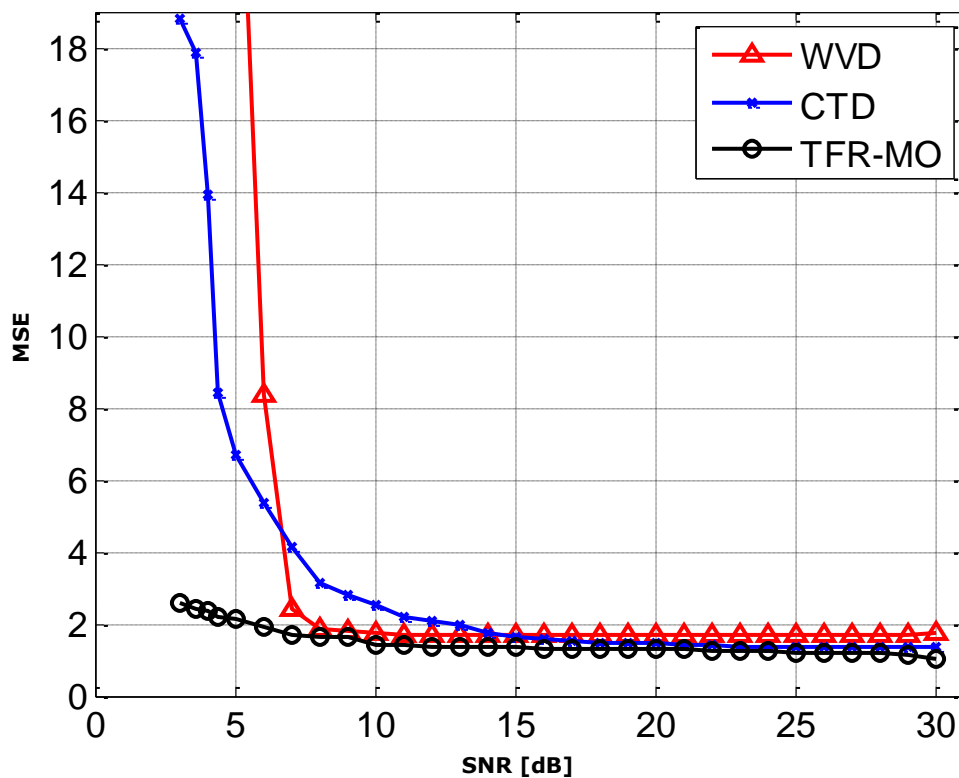


Figura 3.7. Performanțele MSE al IF în raport cu SNR, exemplul 1

Se observă apropierea foarte mare a curbelor de performanță corespunzătoare, în intervalul [14, 30]dB. Odată cu descreșterea SNR, erorile de estimare a frecvenței instantanee MSE pentru WVD și CTD cresc mult mai rapid decât în cazul TFR-MO. Pentru niveluri SNR mai mici de 6dB, metoda TFR-MO furnizează de departe cea mai precisă estimare a IF. Performanțele globale mai bune ale metodei TFR-MO își găsesc un suport în proprietățile operatorilor morfologici utilizați în algoritmul de determinare a vârfurilor din imaginea RTF.

Acestea fiind spuse, rezultatele obținute (figura 3.7) pentru semnale a căror IF prezintă un grad mai mare de neliniaritate, confirmă concluziile rezultate din [BNI05] în ceea ce privește robustețea la zgomot precum și capacitatea de reconstrucție a curbei IF pentru niveluri ale zgomotului foarte ridicate.

Exemplul 2

Al doilea semnal de test considerat, cu IF având o caracteristică extrem de neliniară, este tot un semnal cu fază polinomială și amplitudine constantă, $s(t)$, înecat de un zgomot gaussian alb, de medie nulă, $n(t)$. Semnalul are expresia:

$$s(t) = \exp\{j(3 \cos(nt) - \cos(3nt) / 2 + \cos(5nt) / 1.5)\} + n(t) \quad (3.13)$$

Secvența alcătuită din 128 de eșantioane, cu t având valori în intervalul $[-1, 1]$, pentru un raport semnal pe zgomot SNR=3dB, este reprezentată în figura 3.8.

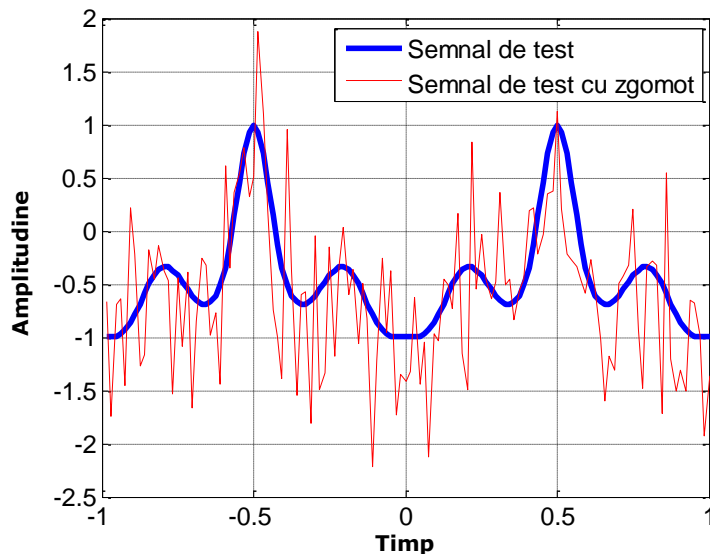


Figura 3.8. Semnal SFP cu amplitudine constantă, cu zgomot gaussian, SNR=3dB, exemplul 2

Frecvența instantanee reală a semnalului de test precum și estimarea ei utilizând metoda TRF-MO, pentru două valori diferite ale raportului semnal pe zgomot (SNR=3dB și SNR=30dB), este ilustrată în figura 3.9. Aceasta demonstrează faptul că pentru acest tip de semnal extrem de nestăționar, abaterea frecvenței instantanee estimate este semnificativă, dominând în eroarea de estimare. Estimatorul IF în acest caz nu poate urmări fidel tranzițiile rapide din semnal. Pe de

altă parte, odată cu creșterea zgomotului, varianța respectiv abaterea suferă o creștere relativ ușoară, ceea ce dovedește încă o dată rezistența la zgomote mari a metodei TRF-MO.

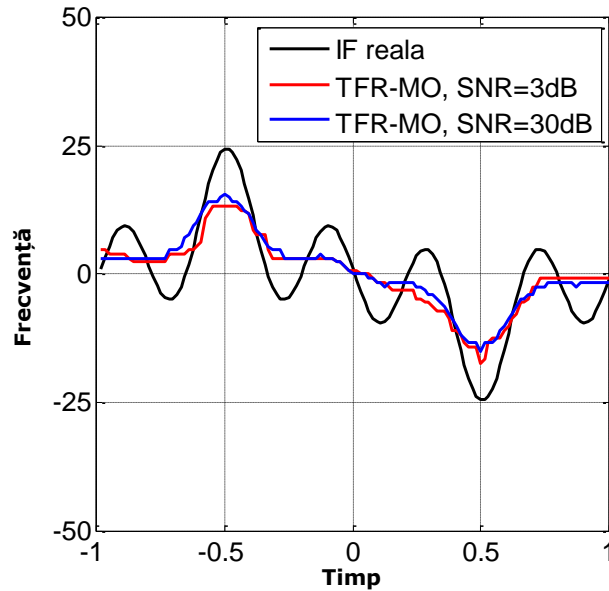


Figura 3.9. Estimarea IF prin metoda TFR-MO, exemplul 2

Figura 3.10 prezintă o comparație a estimării IF între transformările WVD, CTD și TFR-MO. Rezultatele obținute sunt redată pentru un raport semnal pe zgomot SNR=3dB și SNR=30dB.

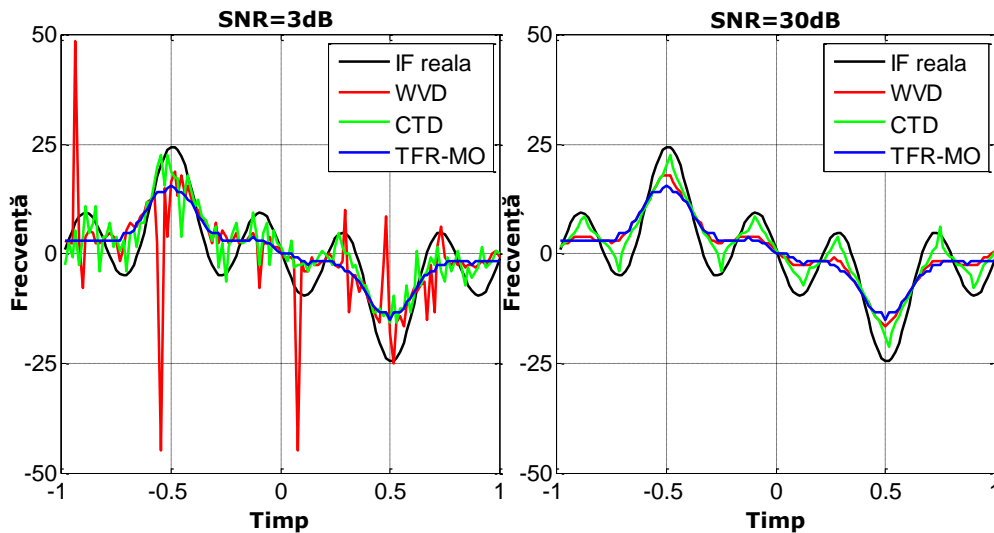


Figura 3.10. Comparație între TRF-MO și câteva reprezentări timp-frecvență, exemplul 2

Se observă că pentru un nivel scăzut de zgomot, abaterea afectează estimarea IF. Cea mai mare abatere se regăsește pentru TFR-MO, în timp ce pentru CTD este mult mai mică, îmbunătățindu-se astfel estimarea globală. Când zgomotul crește, pentru WVD numărul momentelor în care estimatorul IF ratează complet curba IF crește. Prin urmare, deși variația de estimare nu ar trebui să fie mare, aceste ratări degradează serios performanțele distribuției. De asemenea, se constată o creștere a variației în cazul CTD, calitatea estimării scăzând. Abaterea și variația estimatorului TFR-MO pentru un raport SNR de 3dB, rămân aproape neschimbate, ceea ce asigură aproximativ aceleași performanțe de estimare.

În tabelul 3.2 sunt prezentate erorile MSE pentru diferite rapoarte semnal pe zgomot. Analiza rezultatelor prezentate ne poate permite să tragem câteva concluzii. Pe de o parte, pentru SNR=30dB și SNR=15dB erorile cele mai mici se obțin pentru CTD, în timp ce pentru TFR-MO și WVD performanțele sunt apropiate, distribuția WVD fiind totuși superioară. Pe de altă parte, pentru SNR=3dB metoda TFR-MO furnizează cea mai bună estimare IF iar WVD, de departe cea mai slabă.

RTF	SNR [dB]	MSE
TFR-MO	3	47.3605
	15	36.7485
	30	33.8038
CTD	3	58.4536
	15	14.3364
	30	12.9187
WVD	3	331.3292
	15	27.7787
	30	28.0505

Tabel 3.2. MSE al IF estimate, exemplul 2

În vederea comparării performanțelor, în cele ce urmează, se efectuează o analiză statistică a celor trei metode analizate, făcută pe 100 de realizări zgomotoase ale semnalului de test pentru SNR cuprins între valorile 3 și 30dB cu un pas de 1dB. Valorile medii al erorilor MSE în funcție de raportul SNR, sunt reprezentate în figura 3.11.

Analizând aceste curbe, se constată că în intervalul [5, 30]dB metoda CTD furnizează cele mai bune performanțe. Sub niveluri de 5dB, eroarea MSE pentru CTD crește extrem de rapid, situație în care performanțele cele mai bune sunt obținute pentru metoda TFR-MO. Între 3dB și 8dB, TFR-MO este superioară distribuției WVD, performanțele devenind mai apropiate în intervalul [8, 30]dB.

Încă o dată, aceste rezultate arată că metoda TFR-MO constituie un instrument foarte adecvat în prelucrarea semnalelor cu SNR scăzut.

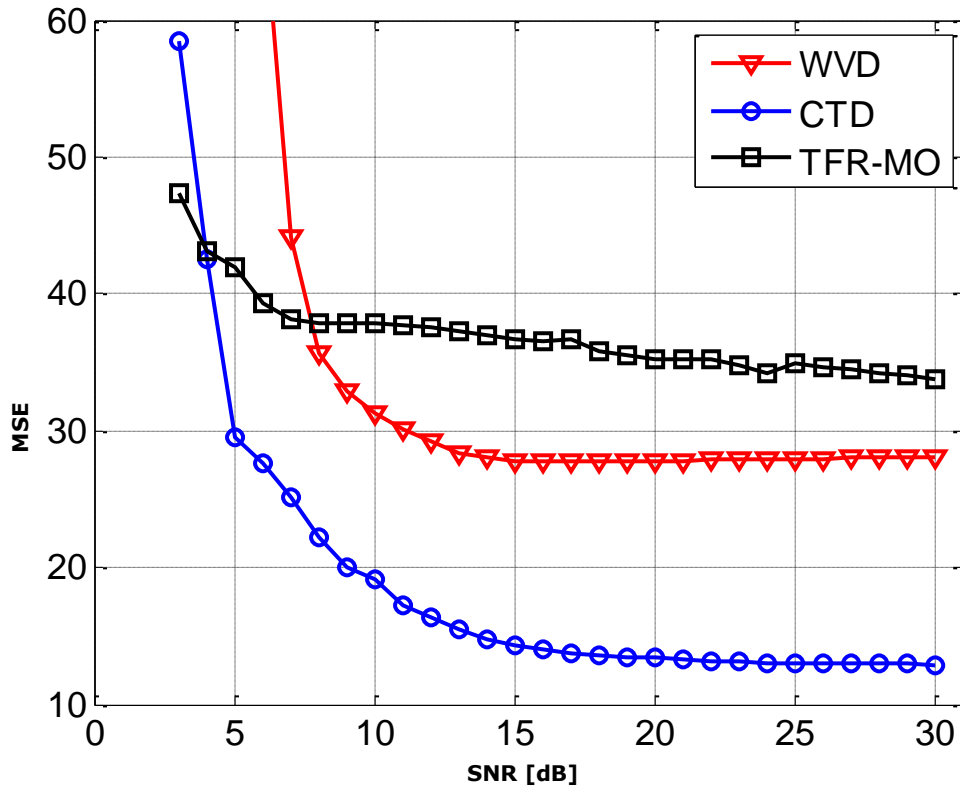


Figura 3.11. Performanțele MSE al IF în raport cu SNR, exemplul 2

În urma simulărilor efectuate, am putut observa că metoda TFR-MO este foarte dependentă de alegerea pragului de filtrare tr . O valoare mică poate determina păstrarea creștelor zgomotului, în afara regiunii planului timp-frecvență unde componenta utilă a semnalului este localizată, precum și păstrarea termenilor de interferență. Acest efect nedorit, este foarte pronunțat pentru un zgomot relativ mare, înrăutățindu-se astfel procesul de estimare. Performanțele pot fi îmbunătățite prin aplicarea operatorilor morfologici doar în regiunea în care este localizată componenta din semnal. Acest lucru poate fi făcut prin tehnici de detecție. În plus, parametrii operatorilor morfologici au un rol important pentru precizia extracției vârfurilor și s-a constatat că pentru rapoarte SNR mari, neaplicarea operatorului morfologic de dilatare în metoda TFR-MO are ca efect îmbunătățirea estimării IF.

O valoare mare a pragului poate cauza întreruperea conectivității în planul timp-frecvență, acest inconvenient putând fi compensat de capacitatea de reconstrucție a operatorilor morfologici. Acest lucru se poate observa din figura 3.10 și figura 3.11, unde pentru un zgomot relativ mare performanțele metodei TFR-MO rămân acceptabile. Totuși, întreruperi mari ale conectivității în planul timp-frecvență pot induce estimări false ale IF.

3.4.2. Semnale multi-componente

Considerăm un semnal de test multi-componente, compus din două componente a căror IF se intersectează în planul timp-frecvență. Componentele din semnal reprezintă o modulație de frecvență parabolică și amplitudine constantă. Semnalul $s(t)$, este înecat de un zgomot gaussian alb, de medie nulă, $n(t)$.

Semnalul are expresia:

$$s(t) = \exp\{j(5\pi t^3 - 9.5\pi t)\} + \exp\{j(-7\pi t^3 + 5\pi t)\} + n(t) \quad (3.14)$$

Secvența alcătuită din 128 de eșantioane, cu t având valori în intervalul $[-1, 1]$, pentru un raport semnal pe zgomot SNR=30dB, este reprezentată în figura 3.12.

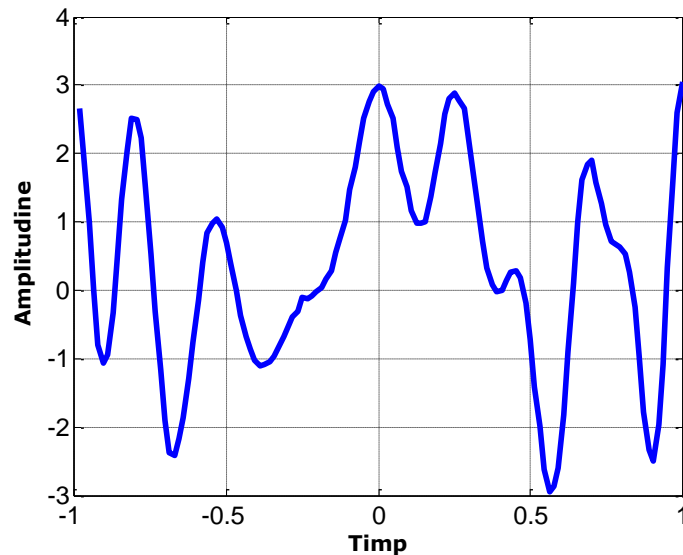


Figura 3.12. Semnal multi-component cu amplitudine constantă, cu zgomot gaussian, SNR=30dB

Frecvența instantanee reală împreună cu estimarea ei utilizând metoda TRF-MO, pentru o valoare SNR=30dB sunt redată în figura 3.13. Se observă din figură, că în ciuda complexității din planul timp-frecvență, variația și abaterea sunt destul de mici. Abaterea este totuși mai mare la intersecțiile componentelor din semnal, unde extragerea unui schelet adecvat este ceva mai dificilă. În plus, calitatea estimării IF cu metoda TFR-MO este influențată de termenii de interferență din WVD.

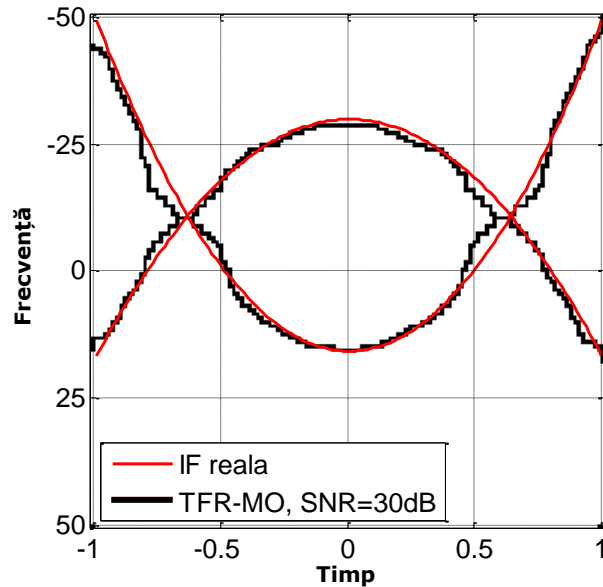


Figura 3.13. Estimarea IF prin metoda TFR-MO, semnal multi-component

3.5. Îmbunătățirea performanțelor TFR-MO

Așa cum am văzut în paragraful 3.4, pentru semnale cu frecvența instantanee puternic neliniară (semnalul cu IF din figura 3.9), datorită abaterilor destul de mari, performanțele metodei TFR-MO sunt mai slabe pentru un raport semnal pe zgomot SNR cuprins între 8dB și 30dB. Performanțele cele mai bune sunt obținute utilizând metoda CTD.

Soluția cea mai bună, care poate să îmbunătățească calitatea estimării IF, este, în mod intuitiv, aceea de a împărți procedura de prelucrare a întregului semnal pe segmente [Sal07], [NS07]. Suportul semnalului de intrare $s(t)$, este divizat în mai multe intervale de lungimi fixe sau diferite, modalitatea de segmentarea fiind specifică semnalului analizat. Se obțin astfel mai multe semnale de intrare. Algoritmul TFR-MO este apoi aplicat pentru fiecare din aceste semnale. În final, estimarea IF rezultă din îmbinarea tuturor curbelor IF estimate corespunzătoare tuturor intervalelor considerate inițial.

Prin urmare, mecanismul propus este bazat pe următorul algoritm secvențial de prelucrare [NS08]:

- 1) Divizarea suportului semnalului de intrare $s(t)$, în mai multe segmente. Pentru fiecare din aceste semnale se aplică următorii pași:
 - Supra-eșantionarea semnalului segmentat.
 - Estimarea IF cu metoda TFR-MO pentru semnalul segmentat supra-eșantionat.
- 2) Estimarea IF globală prin concatenarea curbelor IF estimate pentru fiecare segment din semnal.

Metoda prezentată anterior am numit-o metoda TFR-MO îmbunătățită (TFR-IMO).

În cele ce urmează sunt prezentate rezultatele simulării care s-au efectuat pentru estimarea IF în prezența zgomotului aditiv și gaussian utilizând algoritmul TFR-IMO. Semnalul de test utilizat este semnalul definit în relația (3.13), semnal folosit și în simulările prezentate în paragraful 3.4.

Pentru acest semnal, segmentarea este făcută în maniera ilustrată în figura 3.14. Suportul semnalului este împărțit într-un număr de 10 intervale de lungimi diferite, după cum urmează:

$I_1=[1, 14]$, $I_2=[15, 24]$, $I_3=[25, 42]$, $I_4=[43, 52]$, $I_5=[53, 64]$, $I_6=[65, 78]$, $I_7=[79, 86]$, $I_8=[87, 106]$, $I_9=[107, 114]$, $I_{10}=[115, 128]$.

Amintim faptul că secvența inițială este alcătuită din 128 de eșantioane iar factorul de supraeșantionare 2.

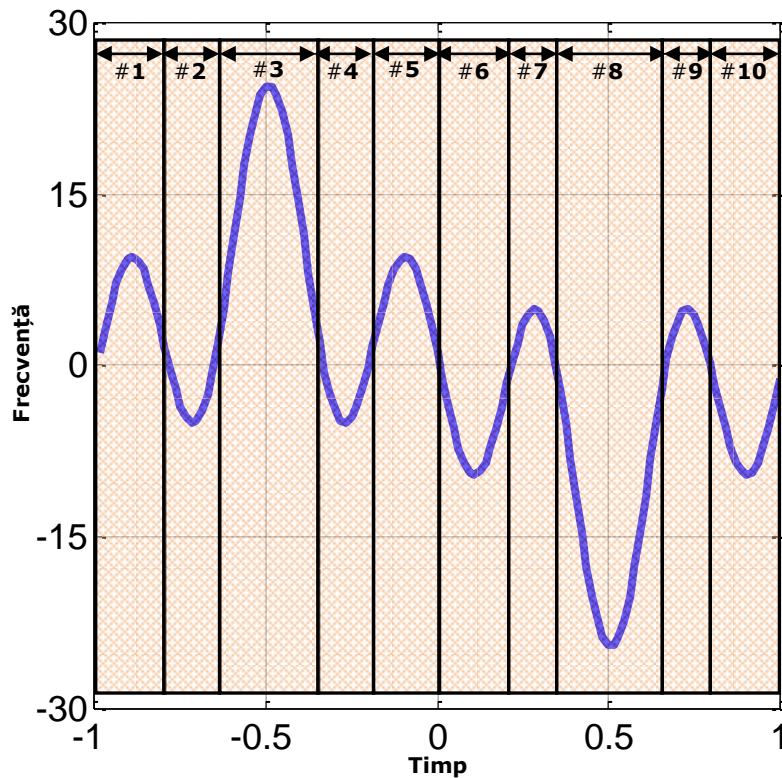


Figura 3.14. Segmentarea suportului semnalului analizat

În figura 3.15 și 3.16, se arată frecvența instantanee estimată, obținută prin metoda TFR-IMO pentru SNR=30dB și SNR=3dB. Se observă, comparativ cu figura 3.9, că abaterea este mult diminuată, estimatorul urmărind mai bine tranzițiile rapide ale IF, ceea ce are ca efect îmbunătățirea performanței de estimare.

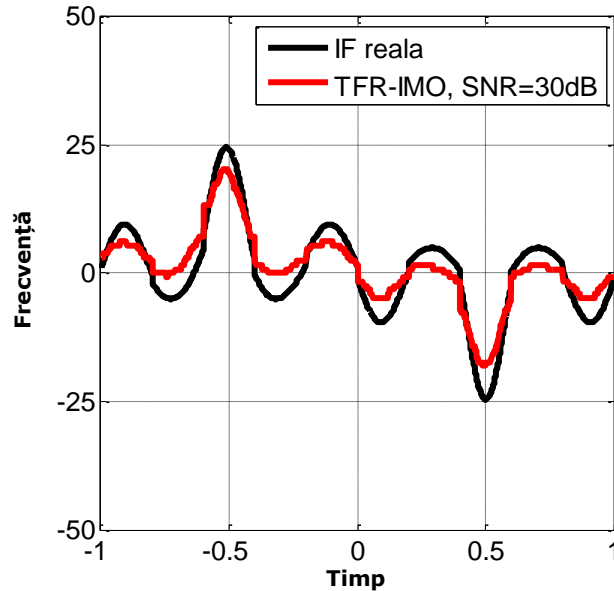


Figura 3.15. Estimarea IF prin metoda TFR-IMO, SNR=30dB, exemplul 2

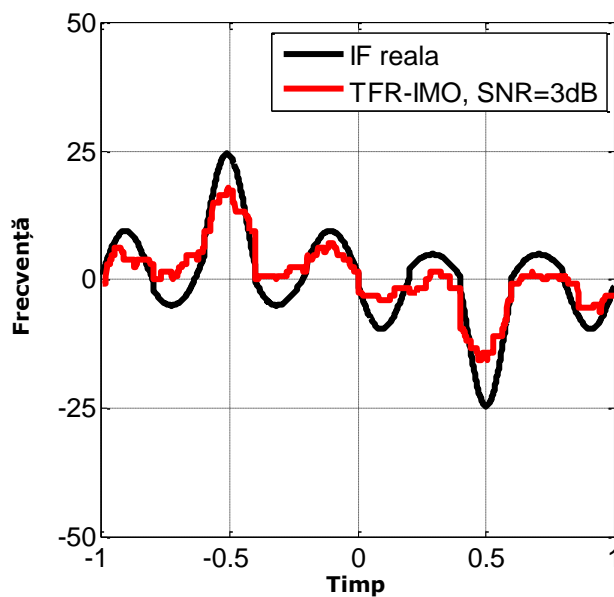


Figura 3.16. Estimarea IF prin metoda TFR-IMO, SNR=3dB, exemplul 2

Erorile MSE obținute sunt redată în tabelul 3.3. Performanța cea mai bună la o anumită valoare a raportului SNR este marcată prin intermediul unui fundal colorat. Ca o remarcă importantă, tabelul 3.3 confirmă îmbunătățirea performanțelor. Astfel, se constată că pentru un raport SNR=30dB, eroarea MSE

pentru TFR-IMO scade de la valoarea 33.8038 (pentru TFR-MO) la valoarea 12.6362 (pentru TFR-IMO).

RTF	SNR [dB]	MSE
TFR-MO	3	47.3605
	15	36.7485
	30	33.8038
TFR-IMO	3	20.9488
	15	13.7383
	30	12.6362

Tabel 3.3. MSE al IF estimate cu metoda TFR-MO și TFR-IMO, exemplul 2

Pentru o analiză mai detaliată a performanțelor TFR-IMO, se repetă analiza statistică efectuată în paragrafele anterioare, calculând valorile medii al erorilor MSE în funcție de raportul SNR, pentru 100 de realizări ale semnalului din relația (3.13), perturbat de zgomot. Rezultatele obținute sunt ilustrate în figura 3.17. Pentru a pune mai bine în evidență performanțele TFR-IMO, în raport cu performanțele metodelor analizate anterior, în figură sunt prezentate și curbele din figura 3.11.

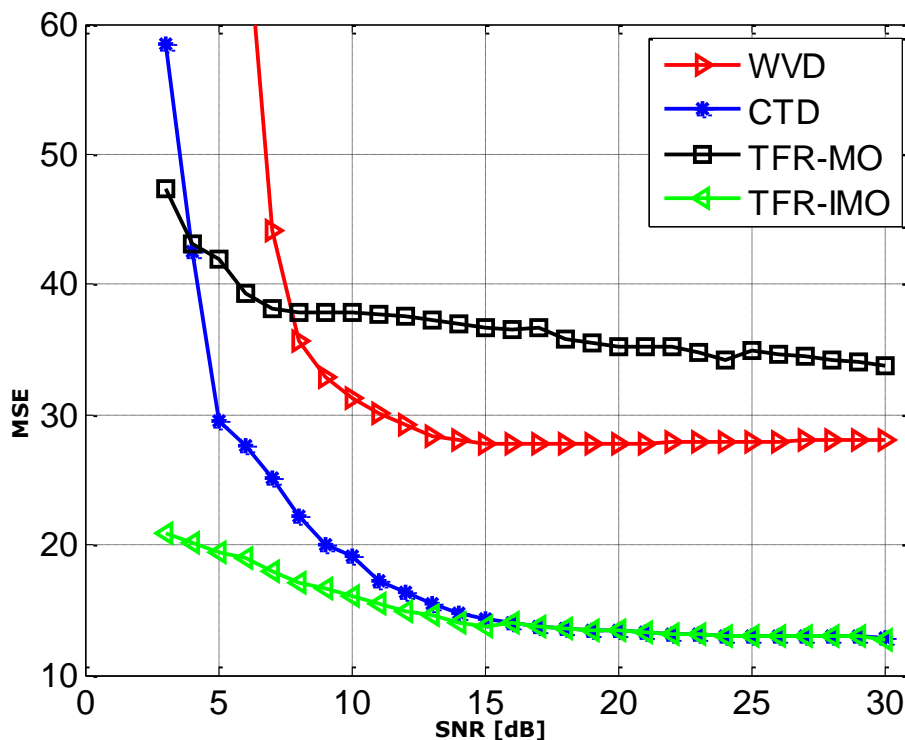


Figura 3.17. Performanțele MSE al IF în raport cu SNR

Analiza curbelor din figura 3.17 dezvăluie câteva concluzii interesante. Astfel, se observă că pentru niveluri ale raportului SNR mai mari de 15dB, performanțele CTD sunt practic egalate de către TFR-IMO, fiind totuși ușor mai bune (12.6362 față de 12.9187, la 30dB). Pe de altă parte, pentru niveluri mici ale SNR, sub 15dB, creșterea erorii MSE este mai pronunțată în cazul CTD, față de cazul TFR-IMO, unde creșterea erorii este mai lentă. Pentru aceste niveluri ale raportului SNR, erorile pentru TFR-IMO sunt sub nivelul celor pentru metoda CTD. Nu în ultimul rând, se constată o îmbunătățire semnificativă a performanțelor TFR-IMO comparativ cu performanțele TFR-MO.

3.6. Concluzii

În acest capitol am efectuat un studiu al performanțelor metodei TFR-MO, pentru semnale cu tranziții rapide ale frecvenței instantanee, comparându-le cu performanțele metodelor WVD și CTD. Utilizând un semnal de test mono-component, cu IF care variază mai lent, rezultatele de estimare cele mai bune se obțin pentru TFR-MO, atât pentru niveluri ridicate cât și pentru niveluri mici ale raportului SNR. Mai exact, din analiza statistică efectuată rezultă că, în intervalul [6, 30]dB performanțele celor trei metode vizate sunt apropiate, diferențe mai mari de performanță în favoarea metodei TFR-MO, înregistrându-se pentru rapoarte de sub 6dB. Rezultatele obținute pentru acest tip de semnale demonstrează robustețea TFR-MO la zgomote mari, lucru confirmat și de autorii din [BNI05], dar pentru semnale cu IF nu foarte neliniare. Pentru un semnal mono-component, cu IF care variază foarte rapid într-un interval scurt de timp, performanțele TFR-MO sunt inferioare metodelor WVD și CTD. Cu toate acestea, pentru un raport SNR=3dB, eroarea MSE pentru TFR-MO este mai mică decât erorile obținute în cazul celorlalte două metode analizate, metoda TFR-MO fiind mai robustă la influența zgomotului. Pentru un semnal multi-component, a cărui componente se intersectează în planul timp-frecvență și cu o variație rapidă a IF, performanțele TFR-MO sunt afectate de către prezența termenilor de interferență. Astfel, la intersecțiile componentelor din semnal unde termenii de interferență sunt mai pronunțați, abaterea este ceva mai mare, ceea ce are ca efect reducerea preciziei estimării globale. În restul planului timp-frecvență, estimatorul TFR-MO prezintă o varianță și o abatere mică. Rezultatele pe care le-am obținut în urma simulărilor, recomandă utilizarea metodei TFR-MO și pentru acest tip de semnale multi-componente.

De asemenea, am propus un nou algoritm secvențial de prelucrare, TFR-IMO, bazat pe metoda TFR-MO. Rezultatelor obținute în urma analizei statistice, confirmă o îmbunătățire semnificativă a performanțelor TFR-IMO comparativ cu performanțele TFR-MO. Se constată o reducere a erorilor MSE de aproximativ două ori și jumătate.

4. DETERMINAREA CELEI MAI BUNE UNDIȘOARE MAMĂ BAZAT PE TEORIA POLINOAMELOR

În prelucrarea semnalelor utilizarea funcțiilor wavelet ("undișoare") constituie deja o tehnică consacrată. Domeniile de aplicare sunt nenumărate: compresie, segmentare, "denoising", "watermarking", transmisii de date, analiza traficului de rețea, etc. Multe dintre aceste tehnici moderne folosesc transformarea DWT. O caracteristică importantă a acestei transformări este capacitatea de a concentra energia semnalului de intrare, într-un număr redus de coeficienți. Astfel, utilizând diferite undișoare mamă se obțin repartiții diferite ale energiei în domeniul DWT. Prin urmare, pentru un semnal de intrare dat, există o undișoară mamă care realizează cel mai bine maximizarea concentrației de energie. De asemenea, această repartiție a energiei între coeficienții wavelet este influențată și de către numărul de iterații DWT. În concluzie, determinarea celei mai adaptate undișoare mamă, permite aproximarea cea mai bună a semnalului original, utilizând un număr minim de coeficienți wavelet.

Scopul acestui capitol este de a prezenta și de a analiza în detaliu, un algoritm nou de determinare a celei mai bune undișoare mamă bazat pe teoria polinoamelor.

4.1. Legătura dintre undișoarele mamă și funcțiile polinomiale

Un semnal $s(t)$, poate fi dezvoltat la fiecare moment de timp t_0 , în serie Taylor, astfel:

$$s(t) = \sum_{k=0}^P \frac{1}{k!} s^{(k)}(t_0)(t-t_0)^k + R_{P+1}(t) \quad (4.1)$$

Relația ne spune că semnalul $s(t)$, se poate aproxima printr-un polinom de grad P , cu t într-un interval I_0 .

În plus, se cunoaște faptul că orice polinom de grad P este un membru al spațiului generat de o analiză multi-rezoluție în $L^2(R)$. Această analiză multi-rezoluție se obține prin utilizarea unei undișoare mamă cu un număr de momente nule mai mare decât P [Daub92]. În [Isar02] autorii demonstrează în plus următoarea afirmație (demonstrația acestei propoziții este redată în anexa 2):

Propoziția 1.

Pentru orice polinom de grad P , numărul cel mai mare de coeficienți de detaliu nuli ai DWT corespunzătoare este obținut atunci când este utilizată o undișoară mamă cu $P+1$ momente nule.

Propoziția 1 este valabilă pentru orice interval din domeniul de definiție al semnalului $s(t)$ inclus în I_0 . Altfel spus, cea mai bună concentrație a energiei pentru orice polinom de grad P , se obține atunci când se folosește o undișoară mamă cu $P+1$ momente nule.

O concentrare bună a energiei, se realizează atunci când rezultă în domeniul DWT cât mai puțini coeficienți cu valoare mare și un număr cât mai mare de coeficienți nuli sau de valoare foarte mică. Prin urmare, în acest caz rezultă aproximarea cea mai bună a semnalului de intrare utilizând un număr minim de coeficienți.

Această proprietate este folosită în aplicații de compresie a semnalelor, [Isar02], sau de "denoising" [Isar04], astfel: se calculează DWT pentru semnalul de intrare, considerat un polinom de grad P folosind o undișoară mamă cu $P+1$ momente nule; se elimină toți coeficienții de detaliu egali cu zero (eventual, se efectuează și o filtrare de tip hard-thresholding pentru eliminarea detaliilor cu valoare foarte mică) și se calculează DWT inversă (IDWT), obținându-se aproximarea semnalului. În acest fel, informația conținută în semnal poate fi recuperată dintr-un număr redus de coeficienți, realizându-se astfel o compresie.

Deoarece în numeroase aplicații nu se cunoaște apriori gradul modelului polinomial care aproximează semnalul de intrare, estimarea lui constituie o provocare majoră la acest tip de aplicații. În [Isar02] estimarea gradului polinomului este făcută cu un algoritm iterativ ce implică o operație de interpolare și o operație de calcul a erorii medii pătratice și a erorii absolute de aproximare pentru diferite grade de polinom. Estimarea gradului funcției polinomiale este obținută prin compararea erorilor cu niște praguri. Acest mecanism este aplicat la compresia semnalelor medicale de tip electrocardiogramă.

Să analizăm în continuare un exemplu. Considerăm un semnal polinomial de gradul 8, alcătuit din 64 de eșantioane, în intervalul $[1, 64]$. Coeficienții polinomului (în ordine descrescătoare a puterilor) sunt: $[-0.00018, 0.013, -0.38, 5.97, -54.31, 288.70, -859.67, 1306.60, -3239.49]$. Rezultatele obținute folosind procedura descrisă mai sus sunt redate în figura 4.1. Astfel, în figura 4.1 (a) se reprezintă semnalul de intrare iar în figura 4.1 (b) avem erorile medii pătratice (MSE) obținute prin interpolarea cu polinoame având gradul de la 1 la 10. Se observă, că eroarea cea mai mică de aproximare se obține pentru un polinom de gradul 9 (marcat în figură printr-un cerc colorat).

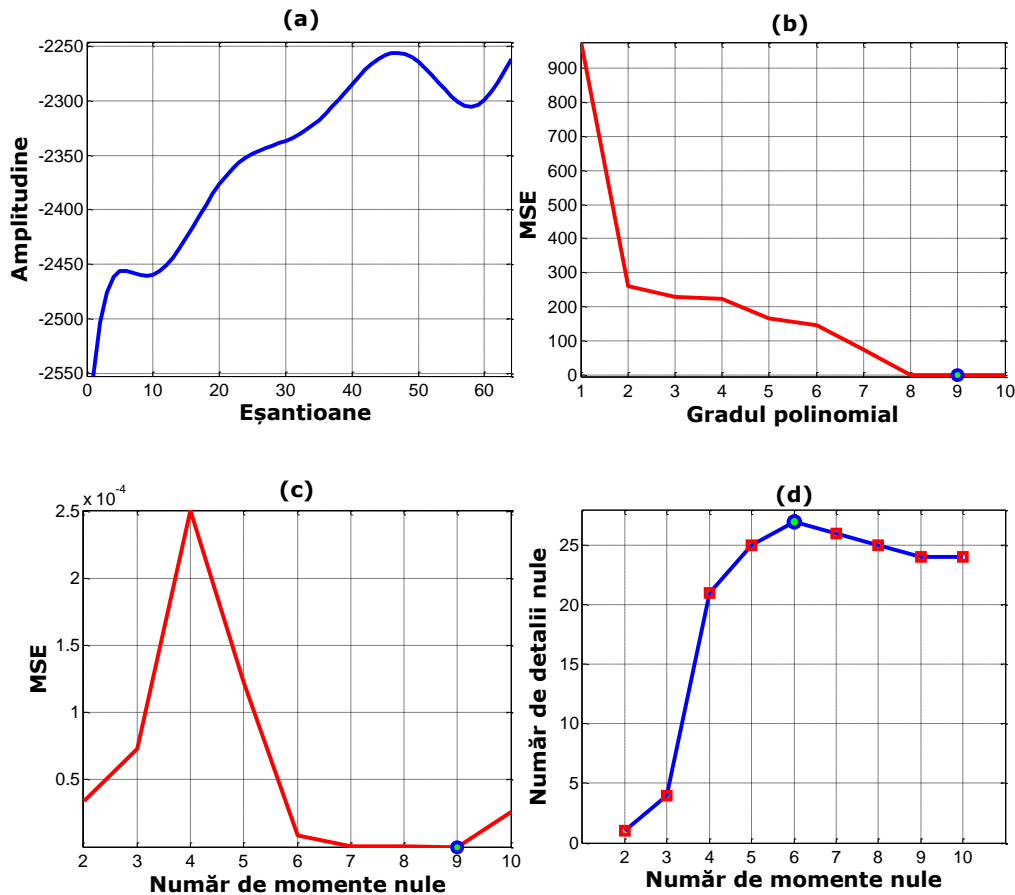


Figura 4.1. Semnal polinomial (a), numărul de detalii nule a undișoarelor (b), eroarea MSE de aproximare în funcție de gradul polinomial de interpolare (c) și în funcție de numărul de momente nule a undișoarelor (d)

Conform, algoritmului popus în [Isar02], undișoara aleasă în procesul de sinteză este undișoara cu 10 momente nule. Totuși, pentru a avea o imagine globală mai completă asupra performanțelor de aproximare, în figura 4.1 (c) sunt redată erorile rezultate prin reconstrucția semnalului utilizând IDWT cu undișoare mamă din familia Daubechies, cu diferite momente nule (de la 2 la 10). Se observă că eroarea cea mai mică este obținută folosind o undișoară mamă cu 9 momente nule. Prin urmare, utilizând o undișoara mamă cu 10 momente nule, nu se obține cea mai bună reconstrucție a semnalului. La fel de bine însă, putem observa din figura 4.1 (b) că se putea considera în estimare un polinom cu gradul 8 sau 10, în funcție de pragurile utilizate. Astfel, dintre aceste trei posibilități, utilizând undișoara mamă cu 9 momente nule se obține performanța cea mai bună.

Pe de altă parte, putem remarca erorile extrem de mici (de ordinul 10^{-4}) în toate cazurile studiate. În plus, am constatat că raportul dintre puterea semnalului reconstruit și puterea semnalului de intrare în toate aceste situații este de 100%,

aproximarea fiind extrem de precisă. La nivel intuitiv, ne punem problema în cele ce urmează dacă nu există cumva o altă undișoară mamă care să fie mai adaptată pentru semnalul considerat. Mai exact, procedura de mai sus, nu garantează faptul că se alege undișoara mamă care asigură, de asemenea, și cea mai bună concentrare a energiei între coeficienții wavelet. În acest sens, în figura 4.1 (d) se prezintă numărul de coeficienți de detaliu nuli obținuți în urma aplicării DWT cu undișoare mamă cu diferite momente nule. Interesant, numărul cel mai mare de detalii nule, 27, se obține pentru undișoara cu 6 momente nule (în figură ilustrat printr-un cerc colorat). Pentru undișoara cu 9 respectiv 10 momente nule se obține un număr mai mic de detalii nule, și anume 24. În concluzie, pentru semnalul considerat, undișoara mamă care realizează cel mai bun compromis între precizia de reconstrucție a semnalului original și numărul minim de coeficienți wavelet utilizați în procesul de sinteză, este undișoara mamă cu 6 momente nule. Încă o observație interesantă, este aceea că pentru semnalul de test primii trei coeficienți corespunzători puterilor cele mai mari sunt foarte mici, prin urmare polinomul poate fi foarte bine aproximat cu un polinom de gradul 5. Așa cum am văzut în figura 4.1 (d), utilizând o undișoară mamă cu 6 momente nule, se obține maximizarea concentrației de putere într-un număr minim de coeficienți.

Soluția cea mai bună, care poate să îmbunătățească rezultatele obținute prin metoda introdusă în [Isar02], are la bază, în mod intuitiv, un principiu ce rezultă direct din propoziția 1 prezentată la începutul acestui paragraf. În acest sens, în [Sal09] am propus o nouă metodă de estimare a gradului polinomului ce aproximează semnalul analizat.

4.2. Algoritmul DWT de estimare a gradului unui polinom

Aproximarea polinomială joacă un rol important în optimizarea proiectării echipamentelor electronice. La rândul lor, metodele de prelucrare bazate pe modelarea polinomială a fazei semnalelor, presupun utilizarea unui ordin polinomial. De cele mai multe ori, pentru astfel de semnale PPS nu se cunoaște apriori ordinul modelului polinomial. În acest sens, în [Sal09] am propus o metodă de estimare a ordinului unui polinom bazată pe strânsa legătură între teoria wavelet și teoria polinoamelor, sub forma unor proprietăți ale DWT.

Metoda alternativă propusă pentru estimarea ordinului unui polinom, are la bază un principiu ce rezultă direct din propoziția 1 de mai sus. Se caută undișoara mamă pentru care se obține DWT cu cei mai mulți coeficienți de detaliu nuli.

4.2.1. Implementare

Schema bloc de prelucrare a algoritmului DWT propus [Sal09], este ilustrată în figura 4.2.

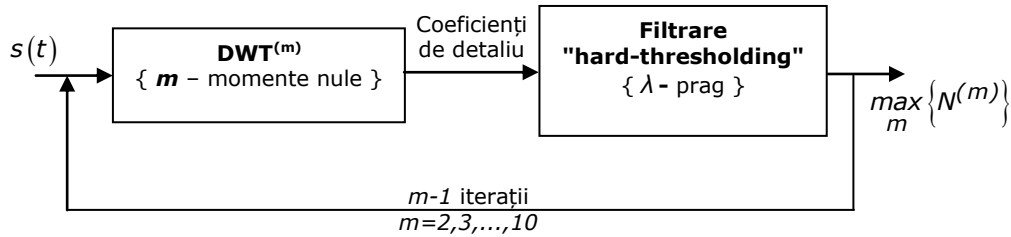
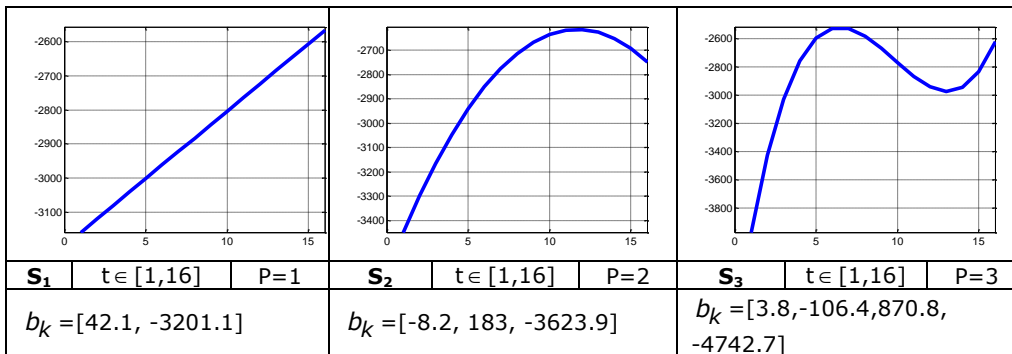


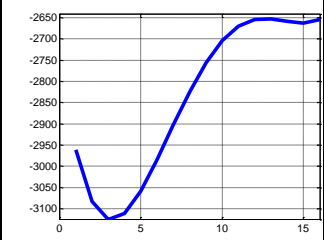
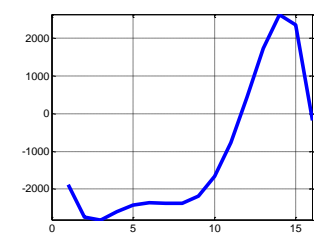
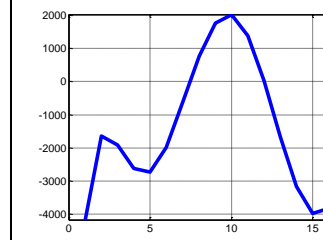
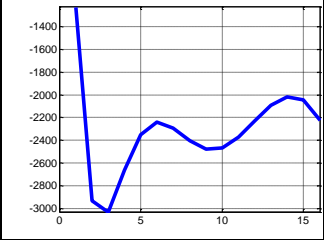
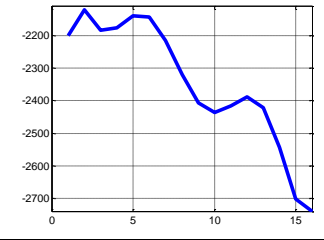
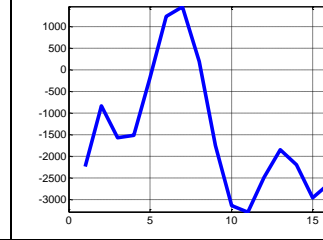
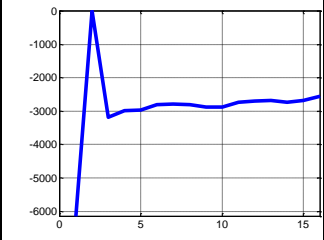
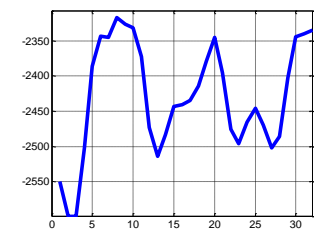
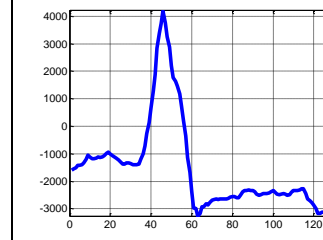
Figura 4.2. Algoritmul DWT de estimare a gradului polinomului ce aproximează un semnal

Pentru semnalul polinomial de intrare $s(t)$ se aplică transformarea DWT, undișoara mamă având m momente nule. DWT generează un set de coeficienți de aproximare și detaliu. În continuare, sunt filtrați doar coeficienții de detaliu prin compararea cu un prag λ . La ieșire se obține astfel, numărul de coeficienți de detaliu nuli, $N^{(m)}$. Algoritmul se repetă iterativ pentru undișoara mamă cu $m = 2, 3, \dots, 10$ momente nule. În final se notează undișoara mamă pentru care s-a obținut cel mai mare număr de coeficienți nuli.

4.2.2. Evaluarea performanțelor pentru câteva tipuri de semnale

O analiză mai riguroasă va fi făcută în cele ce urmează. Întrucât scopul nostru este să arătăm validitatea metodei DWT bazată pe proprietatea definită în propoziția 1, vom considera o serie de semnale de test având caracteristici variate. Parametri de simulare, precum și forma acestor semnale sunt prezentate în figura 4.3. Observăm din figură, de la semnale simple (semnale cu o variație lentă în timp) până la semnale complexe (semnale cu variații rapide pe intervale scurte de timp, cu multe minime și maxime locale). Primele nouă semnale sunt semnale polinomiale, și au fost generate pe baza unor coeficienți b_k . Ultimele trei semnale sunt segmente dintr-un semnal medical de tip electrocardiogramă.



		
S₄ t ∈ [1,16] P=4	S₅ t ∈ [1,16] P=5	S₆ t ∈ [1,16] P=6
$b_k = [0.1, -5.9, 76.3, -316.6, -2714.8]$	$b_k = [-1.3 \cdot 10^{-5}, 0.003, -0.3, 13.8, -219.5, -1667.3]$	$b_k = [-3.4 \cdot 10^{-7}, 10^{-4}, -0.02, 1.7, -57.7, 751.2, -4861.4]$
		
S₇ t ∈ [1,16] P=7	S₈ t ∈ [1,16] P=8	S₉ t ∈ [1,16] P=9
$b_k = [-1.3 \cdot 10^{-7}, 3.8 \cdot 10^{-5}, -0.004, -8.2, 138.5, -1040.9, -320.5]$	$b_k = [-4.1 \cdot 10^{-9}, 1.1 \cdot 10^{-6}, -0.0001, 0.007, -0.2, 4.5, -41, 159.7, -2323.2]$	$b_k = [-5.9 \cdot 10^{-12}, 3.1 \cdot 10^{-9}, -6.7 \cdot 10^{-7}, 7.3 \cdot 10^{-5}, -0.004, 0.1, 0.08, -44.8, 556.3, -2751.9]$
		
S₁₀ t ∈ [1,16] P nedefinit	S₁₁ t ∈ [1,32] P nedefinit	S₁₂ t ∈ [1,128] P nedefinit

Tabel 4.1. Parametrii de simulare a semnalelor de test utilizate în evaluarea performanțelor DWT de reconstrucție

Rezultatele simulărilor sunt redată în tabelul 4.2. În tabelul 4.2, N_d reprezintă numărul de coeficienți de detaliu DWT nuli rezultați. Pentru evaluarea performanțelor de aproximare a semnalului de intrare, am considerat două mărimi: eroarea medie pătratică (MSE) și raportul în procente dintre puterea coeficienților wavelet filtrați (P_f) și puterea tuturor coeficienților wavelet (P_i). Numărul de iterații DWT considerat este egal cu 1.

Așa cum am văzut, conform algoritmului DWT prezentat în figura 4.2, pentru semnalul de intrare, se calculează DWT utilizând undișoare mamă cu diferite

48 Determinarea celei mai bune undișoare mamă bazat pe teoria polinoamelor - 4

momente nule. În simulările efectuate, familia de undișoare mamă folosite sunt cele din familia Daubechies (Daubechies-4, 6, 8, 10, 12, 14, 16, 18, 20). De asemenea, filtrarea de tip hard-thresholding din figura 4.2 a fost ignorată. Algoritmul identifică, undișoara mamă pentru care s-a obținut cel mai mare număr de coeficienți de detaliu nuli. Această undișoară, este apoi utilizată în procesul de reconstrucție a semnalului original, asigurându-se astfel cea mai bună concentrare a energiei într-un număr minim de coeficienți, reconstrucția semnalului inițial fiind în acest caz cea mai bună. Pentru a valida această ipoteză, în cazurile undișoarelor mamă pentru care a rezultat un număr mai mic de detalii nule, am efectuat, în plus, o filtrare a celor mai mici coeficienți de detaliu. În urma acestor operații, pentru toate cazurile undișoarelor analizate vom avea același număr de coeficienți de detaliu nuli, egal cu $\max\{N_d\}$. Performanța cea mai bună de aproximare pentru fiecare semnal analizat este marcată prin intermediul unui fundal colorat.

S	Undișoara mamă	N_d	MSE	P_r / P_i (%)	S	Undișoara mamă	N_d	MSE	P_r / P_i (%)
S ₁	Daub4	7	2.5·10⁻¹⁷	100	S ₂	Daub4	0	29.8	99.9996
	Daub6	6	362.96	99.9955		Daub6	6	1.7·10⁻¹⁵	100
	Daub8	5	805.28	99.9902		Daub8	5	100.3	99.9987
	Daub10	4	624.96	99.9924		Daub10	4	181.9	99.9977
	Daub12	3	135.16	99.9983		Daub12	3	33.7	99.9995
	Daub14	2	104.42	99.9987		Daub14	2	79.8	99.9990
	Daub16	1	974.72	99.9881		Daub16	1	636.4	99.9921
	Daub18	0	1920.60	99.9766		Daub18	0	1533.5	99.9811
	Daub20	0	2127.47	99.9741		Daub20	0	1398.7	99.9828
S ₃	Daub4	0	379.9	99.9954	S ₄	Daub4	0	17.3	99.9997
	Daub6	0	35.3	99.9995		Daub6	0	6.3	99.9999
	Daub8	5	6.4·10⁻¹⁷	100		Daub8	0	0.6	100
	Daub10	4	77.4	99.9990		Daub10	5	0.000101	100
	Daub12	3	75.5	99.9991		Daub12	3	3.8	100
	Daub14	2	18.3	99.9997		Daub14	3	8.8	99.9998
	Daub16	1	344.3	99.9959		Daub16	2	2.1	100
	Daub18	0	1666.7	99.9801		Daub18	1	3.7	100
Daub20	0	3373.1	99.9598	Daub20	0	34.6	99.9995		
S ₅	Daub4	0	2249.4	99.9501	S ₆	Daub4	0	1020.6	99.9828
	Daub6	0	502.4	99.9888		Daub6	0	2270.1	99.9618
	Daub8	0	321.3	99.9928		Daub8	0	137.2	99.9976
	Daub10	0	86.6	99.9980		Daub10	0	149.2	99.9974
	Daub12	3	1.1·10⁻¹⁷	100		Daub12	0	109.4	99.9981
	Daub14	2	0.4	100		Daub14	2	2.9·10⁻¹⁷	100
	Daub16	1	6.1	99.9998		Daub16	1	6.6	99.9998

4.2 – Algoritmul DWT de estimare a gradului unui polinom 49

S	Undișoara mamă	N _d	MSE	P _r / P _i (%)	S	Undișoara mamă	N _d	MSE	P _r / P _i (%)
	Daub18	0	8.4	99.9998		Daub18	0	15.2	99.9997
	Daub20	0	8.8	99.9998		Daub20	0	164.8	99.9972
S ₇	Daub4	0	54.9	99.9990	S ₈	Daub4	0	1.6·10⁻¹⁷	100
	Daub6	0	7.03	99.9998		Daub6	0	1.1·10 ⁻¹⁵	100
	Daub8	0	0.004	100		Daub8	0	4.2·10 ⁻¹⁷	100
	Daub10	0	0.1	100		Daub10	0	8.7·10 ⁻¹⁷	100
	Daub12	0	1.03	100		Daub12	0	4.8·10 ⁻¹⁷	100
	Daub14	0	1.3	100		Daub14	0	8.2·10 ⁻¹⁷	100
	Daub16	1	2.4·10⁻¹⁶	100		Daub16	0	2.5·10 ⁻¹⁶	100
	Daub18	0	0.3	100		Daub18	0	1.5·10 ⁻¹⁶	100
	Daub20	0	0.5	100	Daub20	0	4.9·10 ⁻¹⁶	100	
S ₉	Daub4	0	6.9·10⁻¹⁸	100	S ₁₀	Daub4	0	2.4·10⁻¹⁷	100
	Daub6	0	4.7·10 ⁻¹⁶	100		Daub6	0	1.7·10 ⁻¹⁵	100
	Daub8	0	1.7·10 ⁻¹⁷	100		Daub8	0	6.3·10 ⁻¹⁷	100
	Daub10	0	3.6·10 ⁻¹⁷	100		Daub10	0	1.2·10 ⁻¹⁶	100
	Daub12	0	1.9·10 ⁻¹⁷	100		Daub12	0	7.0·10 ⁻¹⁷	100
	Daub14	0	3.3·10 ⁻¹⁷	100		Daub14	0	1.1·10 ⁻¹⁶	100
	Daub16	0	1.0·10 ⁻¹⁶	100		Daub16	0	3.7·10 ⁻¹⁶	100
	Daub18	0	6.4·10 ⁻¹⁷	100		Daub18	0	2.3·10 ⁻¹⁶	100
	Daub20	0	2.3·10 ⁻¹⁶	100	Daub20	0	7.2·10 ⁻¹⁶	100	
S ₁₁	Daub4	0	0.05	100	S ₁₂	Daub4	0	0.01	100
	Daub6	0	0.04	100		Daub6	1	1.5·10 ⁻⁵	100
	Daub8	0	0.003	100		Daub8	0	0.0009	100
	Daub10	0	0.01	100		Daub10	1	1.3·10⁻⁹	100
	Daub12	0	0.01	100		Daub12	0	0.01	100
	Daub14	0	0.00021	100		Daub14	0	0.002	100
	Daub16	0	0.1	100		Daub16	0	0.004	100
	Daub18	0	0.2	100		Daub18	0	0.02	100
	Daub20	1	1.4·10⁻⁵	100	Daub20	1	3.5	100	

Tabel 4.2. Performanțele de aproximare pentru metoda DWT pentru semnalelor de test din tabelul 4.1

Analiza rezultatelor prezentate ne poate permite să tragem câteva concluzii interesante. Pe de o parte, se poate vedea că pentru semnalele pentru care algoritmul a identificat cel puțin o undișoară cu coeficienți de detaliu nuli, folosind undișoara cu număr maxim de detalii nule, se obține eroarea de aproximare MSE cea mai mică și puterea conținută în coeficienții wavelet (de aproximare și de

detaliu) cea mai mare. În aceste cazuri, erorile MSE sunt de ordinul 10^{-4} (cea mai mare) și 10^{-18} , datorită erorilor inerente de calcul (cea mai mică), iar raportul $\frac{P_r}{P_i}$ de 100 %. Pe de altă parte, se observă că pentru semnalele S_8 , S_9 , și S_{10} , algoritmul nu a identificat nici o undișoare mamă care să genereze cel puțin un coeficient de detaliu zero. Analizând mai atent aceste semnale (tabelul 4.1), putem constata că ele prezintă foarte multe variații rapide pe un interval scurt de eșantioane (semnalele având lungimea de 16 eșantioane). Cu alte cuvinte, pentru astfel de semnale ar fi utilă o supraeșantioanare.

O altă observație interesantă este aceea că, pe măsură ce gradul semnalului polinomial crește, scade numărul maxim de coeficienți nuli obținuți. Astfel, pentru semnale cu variație lentă, se poate realiza cea mai bună compresie și cea mai bună reconstrucție. Nu în ultimul rând, se observă că pentru semnalele de lungime scurtă S_8 , S_9 , și S_{10} , performanțele de aproximare cele mai bune s-au obținut pentru undișoara Daubechies4, care are o localizare mai bună în timp. Totuși, pentru semnalele S_{11} , S_{12} , care sunt de asemenea semnale cu variații multiple și rapide, dar cu o lungime mai mare, undișoarele optime identificate au un număr de momente nule mai ridicat, 10 respectiv 5, pentru care localizarea în frecvență este mai bună. În concluzie, putem afirma că metoda propusă asigură determinarea celei mai bune undișoare: reconstrucție cu o precizie ridicată și un număr redus de coeficienți.

4.2.3. Efectul filtrării coeficienților wavelet de detaliu diferiți de zero

Am văzut în paragraful precedent că pentru anumite semnale, a căror curbe sunt caracterizate de variații rapide, undișoarele mamă considerate nu sunt foarte adaptate, acestea generând foarte puține detalii nule sau în cel mai rău caz, niciunul. O soluție, ar fi utilizarea unor undișoare mamă cu mai multe momente nule. Pe de altă parte, suntem interesați în continuare, de a identifica între undișoarele folosite în algoritmul propus, undișoara mamă care realizează în același timp cea mai bună compresie și cea mai bună aproximare a semnalului de intrare.

Dar să ne amintim, că în simulările efectuate anterior, etapa de filtrare de tip hard-thresholding din figura 4.2 a fost ignorată. Prin urmare, pentru aceste cazuri conform algoritmului propus în figura 4.2, se realizează și o etapă de filtrare a coeficienților de detaliu, utilizând un prag λ . Astfel, undișoara mamă care furnizează cel mai mare număr de detalii nule, va fi undișoara aleasă pentru reconstrucția semnalului analizat. În continuare, pentru evaluarea performanțelor procedurii propuse, am utilizat mai multe valori ale pragului de filtrare λ . Pentru fiecare din aceste praguri, dorim să vedem dacă într-adevăr undișoara mamă selectată astfel, oferă cea mai bună reconstrucție și compresie a semnalului analizat.

Primul semnal de test utilizat este semnalul S_9 , introdus în paragraful 4.2.2, un semnal polinomial foarte nestaționar, compus din $N=16$ eșantioane. Rezultatele obținute în urma simulărilor sunt redată în tabelul 4.3. Cu d_k , s-au notat coeficienții DWT de detaliu.

Mărimă	Daub4	Daub6	Daub8	Daub10	Daub12
Prag: $\lambda = \max\{d_k\} / (N / 2)$					
N_d	1	0	2	2	1
MSE	$2.49 \cdot 10^3$	$2.22 \cdot 10^3$	$0.21 \cdot 10^3$	$0.43 \cdot 10^3$	$1.52 \cdot 10^3$
$P_r/P_i(\%)$	99.9413	99.9475	99.9949	99.9898	99.9640
	Daub14	Daub16	Daub18	Daub20	
Prag: $\lambda = \max\{d_k\} / (N / 2)$					
N_d	1	1	2	1	
MSE	$2.41 \cdot 10^3$	$2.50 \cdot 10^3$	$0.05 \cdot 10^3$	$0.20 \cdot 10^3$	
$P_r/P_i(\%)$	99.9431	99.9411	99.9987	99.9952	
	Daub4	Daub6	Daub8	Daub10	Daub12
Prag: $\lambda = \max\{d_k\} / (N / 6)$					
N_d	3	3	3	4	5
MSE	$3.43 \cdot 10^4$	$2.38 \cdot 10^4$	$1.77 \cdot 10^4$	$1.26 \cdot 10^4$	$0.99 \cdot 10^4$
$P_r/P_i(\%)$	99.1922	99.4379	99.5833	99.7016	99.7653
	Daub14	Daub16	Daub18	Daub20	
Prag: $\lambda = \max\{d_k\} / (N / 6)$					
N_d	3	1	5	4	
MSE	$2.02 \cdot 10^4$	$1.39 \cdot 10^4$	$0.29 \cdot 10^4$	$0.53 \cdot 10^4$	
$P_r/P_i(\%)$	99.5240	99.6719	99.9306	99.8749	
	Daub4	Daub6	Daub8	Daub10	Daub12
Prag: $\lambda = \max\{d_k\} / (N / 10)$					
N_d	6	3	5	6	6
MSE	$7.36 \cdot 10^4$	$5.81 \cdot 10^4$	$4.79 \cdot 10^4$	$4.47 \cdot 10^4$	$4.90 \cdot 10^4$
$P_r/P_i(\%)$	98.2659	98.6326	98.8716	98.9466	98.8457
	Daub14	Daub16	Daub18	Daub20	
Prag: $\lambda = \max\{d_k\} / (N / 10)$					
N_d	5	6	7	6	
MSE	$4.76 \cdot 10^4$	$3.28 \cdot 10^4$	$1.14 \cdot 10^4$	$1.32 \cdot 10^4$	
$P_r/P_i(\%)$	98.8778	99.2259	99.7296	99.6884	

Tabel 4.3. Selecție a performanțelor de aproximare a semnalului de test S_9 , pentru diferite praguri de filtrare

Analiza rezultatelor din tabelul 4.3 dezvăluie câteva concluzii interesante. Semnalul studiat este un polinom de gradul 9. Propoziția 1 indică folosirea undișoarei mamă Daubechies20. Conform tabelului rezultatele obținute folosind această undișoară mamă se află pe locul 2, fiind depășite doar de rezultatele obținute folosind undișoara mamă Daubechies18, indiferent de valoarea pragului lambda. O altă observație este aceea că, cu cât numărul de coeficienți eliminați este mai mare cu atât eroarea MSE crește iar raportul $\frac{P_r}{P_i}$ scade. Pentru a aprecia mai bine vizual calitatea aproximării semnalului, în figura 4.2 sunt ilustrate semnalele de aproximare obținute utilizând undișoara mamă Daubechies18, determinată pe baza algoritmului propus, cu $N_d=2$, respectiv $N_d=7$ coeficienți nuli.

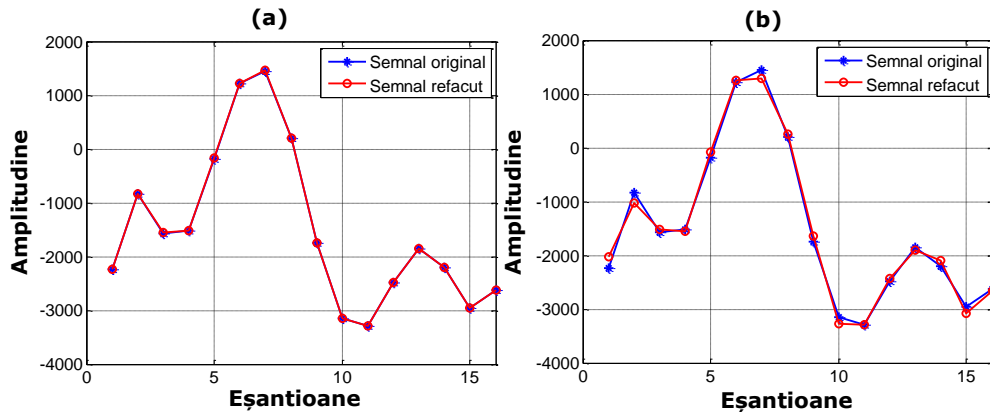


Figura 4.3. Semnalul S_9 reconstruit utilizând undișoara Daubechies18, cu $N_d = 2$ (a), și $N_d = 7$ (b)

Din figura 4.3 (a) și (b), se poate vedea că eliminarea unui număr mic de coeficienți diferiți de zero nu are nici un efect asupra calității aproximării, semnalul refăcut se suprapune practic peste semnalul original, în timp ce eliminarea unui număr mare de coeficienți are ca efect apariția abaterilor, calitatea aproximării fiind în acest caz mai slabă.

Al doilea semnal de test utilizat este semnalul S_{11} , un semnal cu o lungime mai mare $N=32$ eșantioane, cu variații foarte mari. Tabelul 4.4 prezintă performanțele obținute.

Mărimă	Daub4	Daub6	Daub8	Daub10	Daub12
Prag: $\lambda = \max\{d_k\} / (N / 0.5)$					
N_d	0	1	1	2	1
MSE	0.31	0.42	0.85	0.03	0.17
$P_r/P_i(\%)$	100	100	100	100	100
	Daub14	Daub16	Daub18	Daub20	
Prag: $\lambda = \max\{d_k\} / (N / 0.5)$					
N_d	1	0	0	2	
MSE	0.29	0.30	2.98	0.01	
$P_r/P_i(\%)$	100	100	99.9999	100	
	Daub4	Daub6	Daub8	Daub10	Daub12
Prag: $\lambda = \max\{d_k\} / (N / 3)$					
N_d	3	4	5	7	4
MSE	15.53	15.09	12.74	3.73	9.28
$P_r/P_i(\%)$	99.9997	99.9997	99.9997	99.9999	99.9998
	Daub14	Daub16	Daub18	Daub20	
Prag: $\lambda = \max\{d_k\} / (N / 3)$					
N_d	2	2	1	4	
MSE	14.29	18.95	25.18	8.71	

$P_r/P_i(\%)$	99.9998	99.9997	99.9996	99.9999	
	Daub4	Daub6	Daub8	Daub10	Daub12
Prag: $\lambda = \max\{d_k\} / (N / 14)$					
N_d	9	14	15	15	15
MSE	309.41	205.32	159.58	123.26	106.98
$P_r/P_i(\%)$	99.9948	99.9965	99.9973	99.9979	99.9982
	Daub14	Daub16	Daub18	Daub20	
Prag: $\lambda = \max\{d_k\} / (N / 14)$					
N_d	14	13	13	13	
MSE	124.14	151.61	157.55	137.62	
$P_r/P_i(\%)$	99.9979	99.9974	99.9973	99.9977	

Tabel 4.4. Selecție a performanțelor de aproximare a semnalului de test S_{11} , pentru diferite praguri de filtrare

În urma rezultatelor din tabelul 4.4 se observă că, datorită faptului că energia este distribuită într-un număr mai mare de coeficienți de detaliu, prin eliminarea unui număr mai mic de coeficienți nenuli, refacerea semnalului inițial este foarte bună pentru toate undișoarele mamă folosite în simulări. În cazul filtrării unui număr mare de detalii, energia concentrată în coeficienții rămași după filtrare este de asemenea într-un procent ridicat (de ordinul 99.99 %). Pentru praguri diferite se obțin undișoare mamă diferite. În acest caz, ar fi mai potrivit să se facă o supraeșantionare urmată de o segmentare a semnalului achiziționat. Apoi pentru fiecare segment ar putea fi aleasă cea mai bună undișoară mamă, folosind propoziția 1.

Din figura 4.4 (b) se vede o abatere mai mare în momentele de timp unde au loc variațiile rapide din semnal.

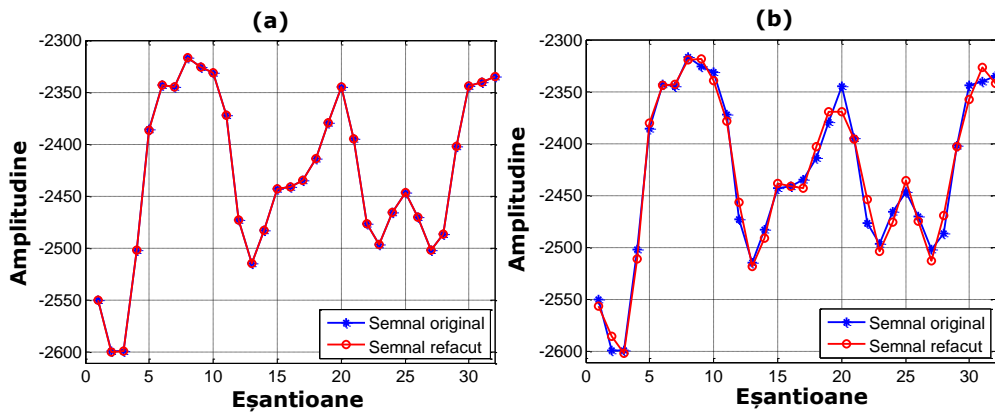


Figura 4.4. Semnalul S_{11} reconstruit utilizând undișoara Daubechies20, $N_d = 2$ (a), și Daubechies12, $N_d = 15$ (b)

Al treilea semnal de test utilizat este semnalul S_{12} , un semnal cu extrem de multe variații rapide, având o lungime mare $N=128$ eșantioane. Performanțele obținute sunt prezentate în tabelul 4.5.

Mărimă	Daub4	Daub6	Daub8	Daub10	Daub12
Prag: $\lambda = \max\{d_k\} / (N / 0.1)$					
N_d	0	1	2	1	0
MSE	0.0269	0.0028	0.0027	0.0032	0.0297
$P_r/P_i(\%)$	100	100	100	100	100
	Daub14	Daub16	Daub18	Daub20	
Prag: $\lambda = \max\{d_k\} / (N / 0.1)$					
N_d	0	0	0	1	
MSE	0.0146	0.0512	0.0858	0.0072	
$P_r/P_i(\%)$	100	100	100	100	
	Daub4	Daub6	Daub8	Daub10	Daub12
Prag: $\lambda = \max\{d_k\} / (N / 4)$					
N_d	19	30	28	31	31
MSE	40.33	27.01	31.76	18.57	13.93
$P_r/P_i(\%)$	99.9992	99.9995	99.9994	99.9996	99.9997
	Daub14	Daub16	Daub18	Daub20	
Prag: $\lambda = \max\{d_k\} / (N / 4)$					
N_d	18	14	15	26	
MSE	31.92	41.13	32.04	21.68	
$P_r/P_i(\%)$	99.9994	99.9992	99.9994	99.9996	
	Daub4	Daub6	Daub8	Daub10	Daub12
Prag: $\lambda = \max\{d_k\} / (N / 64)$					
N_d	62	63	63	63	63
MSE	$2.24 \cdot 10^3$	$1.65 \cdot 10^3$	$1.81 \cdot 10^3$	$1.69 \cdot 10^3$	$1.41 \cdot 10^3$
$P_r/P_i(\%)$	99.9554	99.9671	99.9640	99.9664	99.9718
	Daub14	Daub16	Daub18	Daub20	
Prag: $\lambda = \max\{d_k\} / (N / 64)$					
N_d	62	59	59	61	
MSE	$1.46 \cdot 10^3$	$2.05 \cdot 10^3$	$2.52 \cdot 10^3$	$2.64 \cdot 10^3$	
$P_r/P_i(\%)$	99.9709	99.9591	99.9498	99.9474	

Tabel 4.5. Selecție a performanțelor de aproximare a semnalului de test S_{12} , pentru diferite praguri de filtrare

Din tabel se vede că prin filtrarea aproape a tuturor coeficienților de detaliu diferiți de zero, se obțin erori MSE mai mari și rapoarte $\frac{P_r}{P_i}$ mai mici. Acest fapt este confirmat și din analiza figurii 4.5 (b), în care se poate observa o abatere mai pronunțată a semnalului aproximat față de semnalul original. În cazul în care, pentru mai multe undișoare mamă se obțin același număr de coeficienți nuli, se alege undișoara cu cele mai multe momente nule. De asemenea, putem constata pentru cele trei valori ale pragului λ considerate, algoritmul asigură obținerea performanțelor cele mai bune de aproximare și compresie a semnalului.

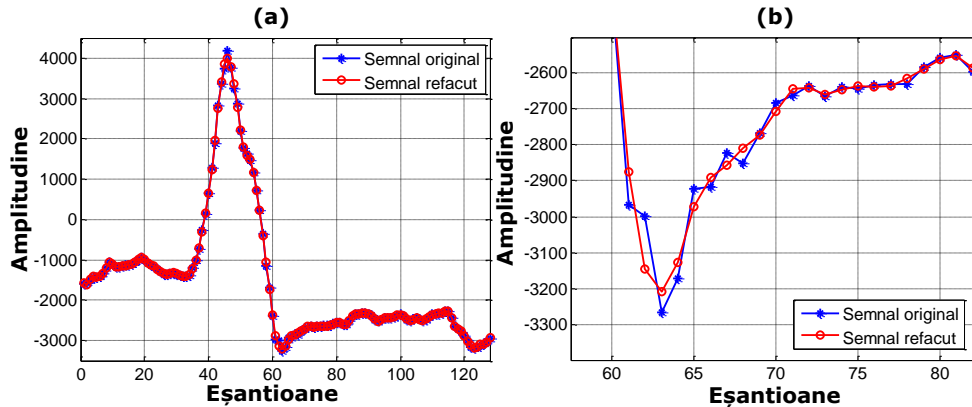


Figura 4.5. Semnalul S_{12} reconstruit utilizând undișoara Daubechies12, $N_d = 63$, în intervalul $[1, 128]$ (a), și în intervalul $[60, 80]$ (b)

Ca o remarcă importantă, rezultatele obținute pentru cele trei semnale de test confirmă validitatea metodei propuse și descrisă în figura 4.2, în determinarea undișoarei mamă optime.

4.2.4. Influența numărului de eșantioane din semnal

Se poate merge mai departe cu analiza algoritmului de determinare a celei mai bune undișoare propus, luând în considerare numărul disponibil de eșantioane din semnal. Așa cum am constatat în paragraful 4.2.2, pentru semnale de lungime mică și cu variații puternice, niciuna din undișoarele mamă considerate nu reprezintă o soluție care să asigure în același timp cea mai bună reconstrucție și compresie a semnalului analizat. În continuare vrem să vedem care este efectul numărului de eșantioane disponibile asupra metodei de selecție a undișoarei mamă.

Primul semnal de test considerat este semnalul S_8 , compus din 16 eșantioane. Rezultatele obținute în urma simulărilor, pentru un număr de eșantioane $N=32, 64, 128$ sunt redată în figura 4.6 și tabelul 4.6. Astfel, în figura 4.6 (a) sunt ilustrate numărul de detalii nule obținute pentru cele 9 undișoare mamă utilizate iar în figura 4.6 (b) erorile de aproximare MSE. Performanțele cele mai bune sunt indicate prin cercuri colorate. De asemenea, tabelul 4.6 conține rezultatele obținute în cele trei cazuri studiate, pentru undișoara mamă selectată de către algoritmul propus.

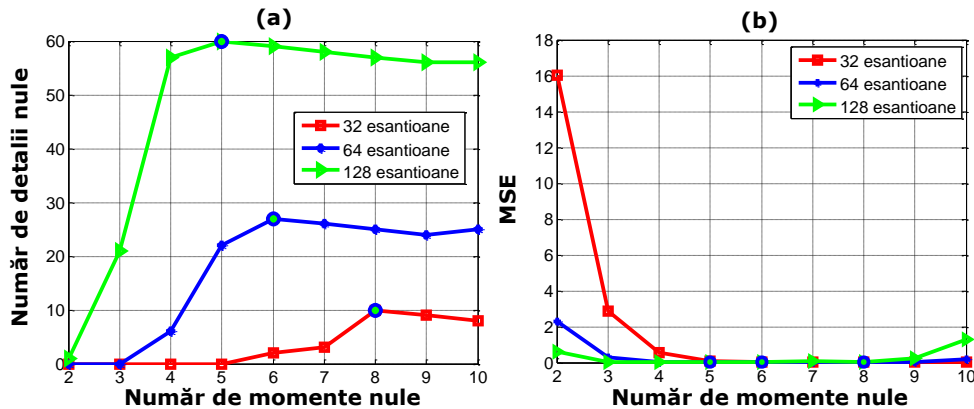


Figura 4.6. Numărul de detalii nule a undișoarelor (a), eroarea MSE de în funcție de numărul de momente nule a undișoarelor (b), pentru semnalul S_8 cu $N=32,64,128$ eşantioane

Număr eşantioane semnal	Undișoara mamă selectată	N_d	MSE	P_r / P_i (%)
$N=32$	Daub16	10	$1.18 \cdot 10^{-4}$	100
$N=64$	Daub12	27	$3.72 \cdot 10^{-5}$	100
$N=128$	Daub10	60	$2.95 \cdot 10^{-6}$	100

Tabel 4.6. Performanțele de aproximare pentru semnalul S_8 , în funcție de numărul de eşantioane disponibile din semnal

Din analiza rezultatelor obținute în urma simulărilor se observă că, odată cu creșterea numărului de eşantioane disponibile din semnal, crește numărul detaliilor nule și scade eroarea de aproximare MSE. Prin urmare, cu cât numărul de eşantioane din semnal este mai mare cu atât mai adaptată va fi undișoara mamă selectată de către algoritmul propus. Propoziția 1 indică undișoara mamă Daubechies18 pentru semnalul S_8 . Conform figurii 4.6 (b) utilizarea acestei undișoare mamă conduce la erori medii pătratice de aproximare foarte mici, indiferent de numărul de eşantioane disponibile. Odată cu creșterea numărului de eşantioane disponibile este posibilă segmentarea semnalului și căutarea celei mai bune undișoare mamă pe fiecare segment.

Al doilea semnal de test considerat este semnalul S_{11} , extrem de variabil și compus din 32 eşantioane. Rezultatele obținute sunt prezentate în figura 4.7 și tabelul 4.7.

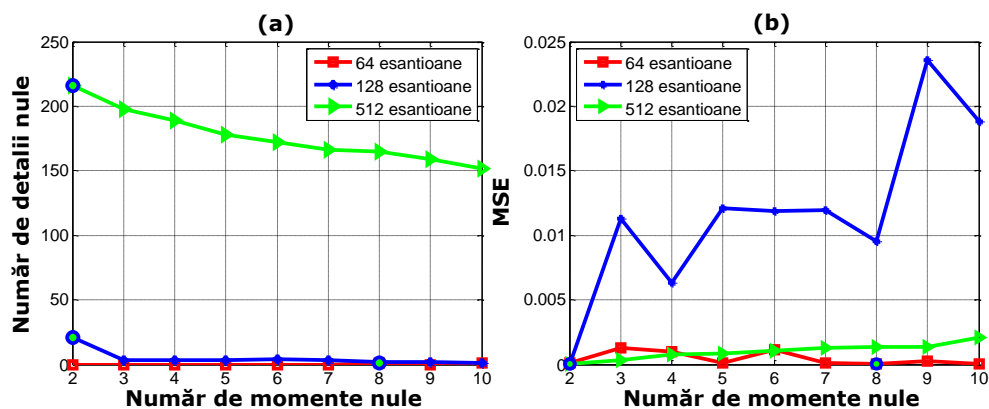


Figura 4.7. Numărul de detalii nule a undișoarelor (a), eroarea MSE de în funcție de numărul de momente nule a undișoarelor (b), pentru semnalul S_{11} cu $N=64,128,512$ eşantioane

Număr eşantioane semnal	Undișoara mamă selectată	N_d	MSE	P_r / P_i (%)
$N=64$	Daub16	1	$1.15 \cdot 10^{-6}$	100
$N=128$	Daub4	21	$2.40 \cdot 10^{-5}$	100
$N=512$	Daub4	216	$6.52 \cdot 10^{-6}$	100

Tabel 4.7. Performanțele de aproximare pentru semnalul S_{11} , în funcție de numărul de eşantioane disponibile din semnal

Rezultatele obținute în acest caz ne conduc înspre aceeași concluzie că, pentru analiza unor semnale cu un număr ridicat de variații rapide, ar fi necesar un număr mai mare de eşantioane din semnal. Acest lucru, ne oferă posibilitatea de a utiliza o undișoară mamă, a cărei coeficienți wavelet au cea mai bună concentrare a energiei semnalului.

5. APLICAȚII ALE RTF ÎN DETECȚIA ANOMALIILOR DIN TRAFICUL DE REȚEA

5.1. Introducere

În prezent, expansiunea tot mai mare a Internetului ca și mediu de comunicare, accesibilitatea on-line a unor informații critice oferită de companii, progresele înregistrate în dezvoltarea tehnologiilor de rețea ce permit foarte ușor conectarea din cele mai îndepărtate puncte ale planetei, acces de la distanță și wireless, servicii web, tehnici de autentificare și criptare, sisteme distribuite de stocare a datelor, etc., precum și vulnerabilitatea acestora, au contribuit decisiv la creșterea fără precedent a activităților cibernetice ilicite și practic toate organizațiile se confruntă cu astfel de atacuri asupra rețelelor și serviciilor pe care le furnizează. Astfel, traficul de rețea malițios, cum ar fi atacuri de tip Denial Of Service (DOS) asupra serviciilor, viruși, viermi, spam-ul, malware-ul, cai troieni, escaladarea privilegiilor, autentificarea neautorizată, injectarea pachetelor nedorite în rețeaua țintă, a devenit o amenințare comună la adresa comunicațiilor din Internet.

Când un calculator este conectat într-o rețea, mai mulți factori contribuie la creșterea riscurilor [Ches94]. În primul rând, crește numărul de locații ce pot servi ca și surse ale unui atac, prin urmare un intrus poate folosi oricare dintre aceste sisteme ce poate transmite pachete acelei stații. În acest context, termenul de intrus este utilizat în descrierea unei persoane care are intenția de a dobândi acces neautorizat la resursele rețelei respective. În plus, anumite servicii trebuie să fie public disponibile, orice calculator din Internet putând fi astfel sursa unor atacuri nedorite. Probabilitatea ca un astfel de lucru să se întâmple este foarte ridicată. Serverele de rețea, pe de altă parte, oferă o gamă largă de posibilități de conectare, de acces a datelor, de transmitere a mesajelor electronice. Toate aplicațiile software ce implementează aceste servicii pot conține bug-uri sau erori de configurare ducând astfel la compromiterea securității.

O serie de studii recente au arătat creșterea complexității și frecvenței atacurilor de rețea, a vulnerabilității aproape inevitabile a aplicațiilor software precum și insecuritatea tot mai ridicată a rețelelor. Aceste fapte au condus la necesitatea dezvoltării unor tehnici de protecție și prevenție.

O soluție clasică pentru diminuarea riscurilor amintite anterior, este utilizarea aplicațiilor de tip firewall și a tehnicilor de criptare. Aplicațiile firewall reprezintă o barieră între zona Internet externă (considerată rețeaua nesigură) și zona de rețea internă (de încredere) din care face parte și sistemul pe care este instalată aplicația firewall. Firewall-ul acționează ca și un punct central ce permite monitorizarea și filtrarea traficului de rețea între aceste două domenii diferite de securitate. Astfel, se minimizează numărul de ținte posibile și se controlează accesul serviciilor publice ce pot fi utilizate.

Tehnicile de criptare, pe de altă parte, împiedică citirea sau modificarea datelor transferate prin rețea. Transmițătorul și receptorul convin asupra unei perechi simetrice sau asimetrice de chei, pentru criptarea (la transmitere) respectiv

decriptarea mesajului (la recepție), prevenindu-se atacurile în timpul tranzitului datelor prin rețea. În plus, pentru o autentificare și mai riguroasă, transmitătorul este autentificat prin folosirea unor mecanisme bazate pe semnătură digitală și pe o autoritate de certificare recunoscută.

Intruziunile în rețea, presupun următoarele etape: etapa de inspecție (supraveghere), etapa de exploatare și etapa de mascare. La început, atacatorul sondează (examinează), strânge și deduce informații sensibile despre sistemele țintă, în efortul de a câștiga accesul neautorizat în sistemele respective și în rețeaua din care fac parte. Apoi, intrusul injectează pachete nedorite în rețeaua țintă, cu scopul de a întrerupe funcționarea normală a serviciilor și comunicației din rețeaua respectivă. În final, atacatorul își ascunde toată activitatea făcută după efectuarea cu succes a intruziunii.

Aceste două strategii descrise mai sus, reprezintă modalități importante pentru îmbunătățirea securității unui sistem din rețea. Cu toate acestea, anumite servicii (cum ar fi serviciile de wide web, de nume de domeniu) trebuie să fie disponibile pentru oricine este conectat la Internet. Prin urmare, acestea nu pot fi blocate de firewall, devenind astfel ținte aproape sigure într-un mediu ostil. Deși instalarea regulată a actualizărilor de sistem este benefică și necesară, s-ar putea ca aceste actualizări ce repară bug-urile descoperite ale aplicațiilor software, să nu fie instalate corect sau în timp util, înainte ca un atacator să exploateze vulnerabilitățile respective.

Este evident faptul că utilizarea doar a criptării și firewall-urilor nu pot asigura protejarea completă a calculatoarelor dintr-o rețea împotriva unor clase de comportamente malițioase. Așadar, este imperios necesar instalarea unei aplicații suplimentare de protecție pentru a recepționa eficient și la timp avertizările privind activitățile malițioase și a face față intruziunilor în cazul unei penetrări a securității.

În ultimii ani, problema detecției intruziunilor într-o rețea a atras puternic atenția în domeniul securității rețelelor. Sistemele ce încearcă detecția comportamentului malițios având ca țintă o rețea și resursele ei sunt numite Sisteme de Detecție a Intruziunilor (IDSs). Un astfel de sistem, strânge și analizează informații de la un calculator anume sau din rețea cu scopul de a identifica posibilele breșe de securitate, în oricare din cele trei etape a unei intruziuni. În mod tradițional, IDS-urile pot fi împărțite în două categorii principale: bazate pe semnătura atacului care caută tipare specifice cunoscute și cele bazate pe anomalii, care detectează anumite deviații de la comportamentul obișnuit. Prin urmare, sistemele de detecție a intruziunilor constituie pe lângă criptare și firewall, cel de-al treilea element de bază în protejarea unui calculator dintr-o rețea.

Rezumând, adoptarea IDS-urilor este motivată de o serie de factori:

1. Studiile au arătat că majoritatea calculatoarelor, indiferent de producător sunt pline de vulnerabilități [Land94], că numărul de incidente de securitate este în continuare foarte ridicat [CERT] și că utilizatorii precum și administratorii de rețea sunt lenți în aplicarea actualizărilor de sistem [Resco03]. În consecință, tot mai mulți experți cred că sistemele nu vor fi niciodată absolut securizate [Bello01].
2. Unele mecanisme de securitate (cum ar fi autentificarea și controlul accesului) pot fi dezactivate datorită erorilor de configurare sau atacurilor malițioase.
3. Utilizatorii de sistem pot abuza de privilegiile lor, efectuând acțiuni dăunătoare.
4. Chiar dacă un atac nu este reușit, în unele cazuri este util să fii avertizat de încercarea de compromitere a securității.

Detecția bazată pe semnătură presupune întreținerea unei baze de date cu toate semnăturile atacurilor cunoscute. Prin analiza pachetelor colectate și a urmelor lăuate în sistem, atacul poate fi identificat. Marele avantaj al unui astfel de sistem îl constituie faptul ca atacurile cunoscute pot fi foarte sigur detectate, cu o rată mică de alerte false. Totuși, aceasta necesită actualizarea frecventă a semnăturilor pentru cele mai noi atacuri identificate. În ceea ce privește dificultățile cu care se confruntă acest tip de detecție putem aminti: identificarea unui atac care cuprinde mai multe pachete și care se întinde pe parcursul mai multor evenimente discrete, detectarea atacurilor noi, încă necunoscute.

Ca și alternativă a detecției bazată pe semnătură, a fost introdusă tehnica bazată pe detecția anomaliilor. Mai întâi, sunt create profilele ale activității normale utilizând diferite măsurători, și apoi o intruzie este detectată de fiecare dată când comportamentul sistemului monitorizat deviază de la profilele de bază stabilite anterior. Unele din beneficiile sistemelor de detecție a anomaliilor sunt: abilitatea de a identifica atacuri necunoscute, capacitatea de a detecta atacuri interne. Cu toate acestea, detecția bazată pe anomalii prezintă la rândul ei și câteva dezavantaje: stabilirea profilului traficului normal este dificilă și poate fi de durată, un profil neadecvat al traficului normal putând duce la performanțe foarte slabe în detecția atacurilor/intruziunilor; numărul mare de alarme false precum și dificultatea ce rezultă din aceasta în determinarea evenimentului ce a declanșat alarma respectivă; un utilizator cu intenții răuvoitoare poate injecta gradat trafic malițios, astfel încât sistemul de detecție a anomaliilor să îl considere ca și trafic normal.

Există o serie de tehnici de detecție folosite în identificarea anomaliilor: detecția statistică, tehnica mașina-de-învățare ("machine learning"), detecția de tip data-mining, etc. Ca o soluție alternativă la metodele tradiționale de detecție a anomaliilor, o serie de tehnici bazate pe prelucrarea de semnal au găsit numeroase aplicații în dezvoltarea IDS-urilor, dintre care recent, tehnicile bazate pe analiza wavelet datorită proprietății lor inerente în domeniul timp-frecvență, de a descompune semnalele în diferite componente la diferite frecvențe.

Această capitol se înscrie în domeniul tehnicilor de aplicare a prelucrării de semnal în dezvoltarea sistemelor de detecție a intruziunilor, mai exact utilizarea analizei wavelet în detecția anomaliilor în traficul de rețea.

5.2. Caracteristici ale IDS-urilor

Sistemele de detecție a intruziunilor (IDSs) sunt niște aplicații software dedicate detecției accesului neautorizat la un calculator sau într-o rețea. IDSs au fost proiectate cu scopul de a completa metodele tradiționale de securitate. Un astfel de sistem de detecție a intruziunilor trebuie să aibe următoarele caracteristici [Dacier99]:

- acuratețe: un IDS nu trebuie să identifice o acțiune legitimă într-un sistem ca fiind o acțiune malițioasă (o acțiune legitimă care este catalogată drept o intruziune se numește alarmă falsă);
- eficiență: eficiența IDS trebuie să fie suficient de ridicată astfel încât detecția intruziunii să se efectueze în timp util, înainte ca prejudiciile să fie semnificative;
- performanță: un IDS trebuie să detecteze toate atacurile sau intruziunile, deziderat aproape imposibil de realizat în practică;
- securitate: un IDS trebuie să fie el însuși securizat împotriva atacurilor;

- scalabilitate: un IDS trebuie să fie capabil să prelucreze un număr cât mai mare de evenimente, fără a elimina informațiile pertinente.
- Conform [Axel98], arhitectura generală a unui sistem de detecție a intruziunilor conține următoarele module:
- **Colectarea datelor:** Acest modul este utilizat pentru strângerea informațiilor din multiple surse: traficul de rețea, antetele (headers) pachetelor, log-urile aplicațiilor etc., acestea urmând să fie analizate prin diferite metode de detecție a intruziunilor.
 - **Stocarea datelor:** În mod obișnuit pentru analize ulterioare, IDSs păstrează datele colectate fie pe o perioadă nedeterminată, fie pe o perioadă suficient de lungă. Deoarece volumul datelor stocate poate să fie foarte mare, scopul principal în proiectarea IDSs este reducerea cât mai eficientă a datelor înregistrate, fără a afecta performanța de detecție.
 - **Analiză și detecție:** Reprezintă blocul central de prelucrare al IDS în care sunt implementați algoritmi de detecție a activităților malițioase. Acești algoritmi se pot clasifica în două mari categorii: bazați pe detecția semnăturilor și cei bazați pe detecția anomaliilor.
 - **Stocarea datelor de referință:** Acest modul salvează informații privind semnăturile atacurilor cunoscute sau profilele comportamentelor considerate normale. Informațiile trebuie să fie actualizate permanent.
 - **Alarma:** Răspunsul furnizat de IDS în ceea ce privește măsura ce trebuie luată în cazul unui eveniment (de ex. generarea unei alerte sau întreprinderea unei acțiuni proactive), este pusă în aplicare de către acest bloc.
- Sistemele IDS pot fi clasificate după o serie de criterii, dintre care, cele mai utilizate sunt [Dacier99]:
- *Tipul de răspuns:* în funcție de răspunsul furnizat de IDS, pot fi pasive sau active. Cele pasive, generează doar o alertă fără a opri atacul detectat și sunt cele mai întâlnite. Acest tip de sistem de detecție necesită intervenția manuală a unei persoane responsabilă cu asigurarea administrării și securității rețelei respective, pentru luarea măsurilor reactive. Prin urmare, pot exista întârzieri în aplicarea acestor măsuri de protecție, ceea ce reprezintă un dezavantaj.
 - *Frecvența de utilizare:* se împart în sisteme dinamice, ce analizează datele stocate în timp real și în sisteme statice, ce analizează offline datele stocate la diferite momente de timp. Un avantaj al prelucrării online îl reprezintă faptul că odată cu detecția unui atac se pot lua măsurile potrivite în timp util, în schimb această metodă poate duce la încărcarea foarte mare a sistemului pe care este instalată aplicația IDS. În schimb, sistemele IDS offline sunt utilizate la analiza "postmortem", care poate fi mult mai amănunțită și completă.
 - *Metoda de detecție:* tradițional există două abordări. În cea bazată pe semnătură, IDS identifică atacul definind care este comportamentul anormal pentru fiecare atac cunoscut, și comparându-l cu acesta. În ceea ce privește metoda bazată pe detecția anomaliilor, IDS stabilește ce este normal și orice abatere, este semnalată ca și posibil atac.
 - *Sursa datelor colectate:* datele care urmează a fi analizate pentru detecția atacurilor, pot proveni din mai multe surse. Astfel, există sisteme IDS care prelucrează datele colectate doar de la un singur calculator, generate de o aplicație specifică sau provenind de la monitorizarea traficului de rețea.
- Caracteristicile ultimelor două criterii de clasificare a sistemelor de detecție a intruziunilor vor fi prezentate în detaliu în paragrafele următoare.

5.3. Metode de detecție

5.3.1. Detecția bazată pe semnătură

Elementul central al sistemelor IDS bazate pe detecția semnăturii atacurilor, îl constituie existența unei baze de date cu informații foarte detaliate privind modelele (semnăturile) atacurilor deja cunoscute. Astfel, datele colectate de IDS sunt comparate cu această bază de date și în cazul unei corespondențe, se generează o alertă sau se execută o măsură reactivă predefinită. Unul din avantajele cele mai importante al unui astfel de sistem IDS îl constituie faptul că se generează extrem de puține alarme false, atacurile fiind indentificate cu o foarte mare precizie. Din păcate, putem identifica și câteva dezavantaje destul de importante. Actualizarea bazei de date de semnături necesită o muncă intensă și dificilă pe de o parte și imposibilitatea detecției atacurilor noi, necunoscute, pe de altă parte.

În funcție de memorarea stărilor unui eveniment malițios, sistemele IDS bazate pe semnătură pot fi diferențiate în două mari categorii: fără înregistrarea stărilor, respectiv cu înregistrarea stărilor.

Un IDS fără memorarea stărilor unui posibil atac, tratează individual fiecare eveniment. Astfel, procesul de analiză se reduce doar la căutarea și identificarea semnăturii evenimentului curent în baze de date, fără a o corela cu informațiile provenind de la alte evenimente anterioare detectate. Prin urmare, această tehnică permite o simplificare semnificativă a proiectării IDS, pentru că nu este necesară păstrarea în memorie a stărilor altor evenimente.

Totuși, aceste sisteme IDS au și limitări importante. În primul rând, ele sunt incomplete, adică nu pot detecta atacurile mai complexe, care necesită mai mulți pași de execuție, fiecare dintre acești pași nefiind în sine malițios și constituind o intruziune doar la execuția completă a lor. În plus, IDS fără înregistrarea stărilor evenimentelor, pot fi supuse unei clase de atacuri care au ca scop declanșarea generării unui număr extrem de mare de alerte, proces numit "inundare" (flood), prin simularea comportamentului atacurilor dintr-o bază de date de semnături, putând duce astfel la blocarea IDS sau ascunderea unor atacuri reale [Stick04], [Snot04].

Sistemele IDS cu memorarea stărilor unui eveniment, datorită faptului că păstrează informații despre evenimentele desfășurate în trecut, permit detecția atacurilor care necesită derularea mai multor pași de execuție. Implementarea unor astfel de sisteme IDS devine mai complexă decât în cazul celor fără memorarea stărilor. În schimb, sistemele IDS cu memorarea stărilor sunt mai puțin predispuse la atacurile de tip "inundare", deoarece este mult mai dificil de a simula cu exactitate modelul unui atac compus din mai mulți pași.

Rezumând, principalele dezavantaje ale sistemelor IDS bazate pe detecția de semnătură sunt următoarele:

- Fiecare atac necesită stocarea unei noi semnături în baza de date, dimensiunea ei putând ajunge foarte mare. De remarcat faptul că același atac poate avea nenumărate versiuni diferite.
- Cu cât semnătura este mai detaliată, cu atât probabilitatea de apariție a alertelor false este mai mică.
- Cu cât semnătura unui atac este mai detaliată și specifică, cu atât este mai ușor pentru un atacator să creeze o versiune modificată a atacului respectiv, acest nou atac nefiind detectat de către IDS.
- În cazul unor atacuri multiple concurente, efortul de calcul al IDS poate fi foarte mare, afectându-se performanțele de detecție ale IDS.

Există un număr mare de sisteme IDS bazate pe semnătură, "open source" sau comerciale, cel mai cunoscut fiind Snort [Snort], dezvoltat inițial de către Martin Roesch în 1998.

5.3.2. Detecția bazată pe anomalii

Ideea fundamentală a tehnicii bazate pe detecția de anomalii, este aceea că o activitate malițioasă este rezultatul unei activități anormale [Kumar94]. Aceste sisteme IDS determină mai întâi modelul comportamentului normal (de ex. profilul sistemului, traficului de rețea, etc.) și apoi identifică evenimentele malițioase, ca fiind acelea care se abat de la comportamentul stabilit anterior. Prin urmare, tot ce este anormal este considerat malițios.

În cazul ideal, activitățile anormale vor fi aceleași cu activitățile malițioase. Cu toate acestea, evenimentele malițioase nu vor coincide tot timpul cu evenimentele anormale. Putem distinge cazurile nefavorabile când evenimentul este malițios dar nu este anormal (sistemul IDS nu detectează intruziunea), sau când evenimentul nu este malițios dar este anormal (sistemul IDS detectează fals o intruziune). Avantajul major al IDS bazate pe anomalii este acela că pot detecta atacuri noi, necunoscute anterior. În schimb, aceste sisteme IDS pot genera un număr mare de alarme false, ceea ce îngreunează munca unui administrator de securitate, care trebuie să investigheze fiecare incident raportat de către IDS și să le elimine.

Există o serie de abordări care au fost propuse pentru detecția anomaliilor: metoda statistică de detecție, metoda de tip "data-mining" sau metoda bazată pe "mașina-de-învățare" (machine learning).

În detecția statistică, sistemul IDS observă comportamentul entității monitorizate și generează profilele rezultate. Aceste profile pot reprezenta diferite măsurători (de ex. gradul de utilizare al procesorului, numărul de conexiuni într-o perioadă, numărul de pachete trimise/receptionate, etc.) și sunt memorate de către sistemul IDS, constituind o referință pentru analizele ulterioare. Astfel, în timpul prelucrării, sistemul IDS actualizează profilele măsurătorilor utilizate, comparând profilele curente cu cele de referință aflate în memorie, prin calcularea unor funcții de cost. Aceste funcții de cost estimează gradul de iregularitate al evenimentului analizat. Dacă costul rezultat este mai mare decât un prag predefinit, sistemul IDS generează o alertă.

Sistemele IDS bazate pe analiza statistică au o serie de avantaje. În principal, aceste sisteme nu necesită cunoașterea apriori a breșelor de securitate sau a atacurilor, fiind astfel capabile de a detecta atacuri de ultimă oră. De asemenea, această tehnică permite identificarea din timp a atacurilor malițioase care se desfășoară pe perioade de timp îndelungate. Un exemplu bun în acest caz ar fi atacurile de tip denial-of-service (DoS), sau de scanare a porturilor.

Cu toate acestea, există și dezavantaje. Dacă în faza de stabilire a profilelor de referință există atacuri malițioase, atunci sistemul IDS le va accepta ca fiind normale, atacurile trecând neobservate. În plus, este destul de dificil de a stabili pragurile optime, pentru a minimiza alertele false pe de o parte, și a detecta cât mai multe atacuri malițioase, pe de altă parte. Acest tip de sisteme IDS au în general performanțe mai puțin bune, din acest punct de vedere [Axel99].

Un alt aspect important, îl constituie faptul că majoritatea sistemelor dintr-o rețea sunt caracterizate de o rată ridicată de schimbare, fiind foarte imprevizibile și caracteristice mediului respectiv. Mai mult decât atât, există numeroase diferențe de

implementare între aplicații precum și ambiguități privind specificațiile protocoalelor. Toate acestea, cresc dificultatea detectării anomaliilor, făcând necesară luarea în calcul a caracteristicii de nestaționaritate a proceselor în alegerea distribuțiilor statistice.

În literatura de specialitate, au fost propuse numeroase tehnici statistice pentru detectarea anomaliilor: analiza spectrală pentru identificarea fluxurilor de date TCP legitime [Cheng02], analiza de tip componentă-principală [Lakhina04], estimarea entropiei maxime [Gu05], filtrarea adaptivă, suma cumulativă [Siris04], [Blazek01], etc.

Ca o soluție alternativă la metodele tradiționale de detecție a anomaliilor, o serie de tehnici bazate pe prelucrarea de semnal au găsit numeroase aplicații în dezvoltarea IDSs, dintre care recent, tehnicile bazate pe analiza wavelet datorită proprietății lor inerente în domeniul timp-frecvență, de a descompune semnalele în diferite componente la diferite frecvențe. Acest subiect este prezentat în detaliu în paragraful 5.7.

5.4. Tipuri de date colectate

Sistemele de detecție a intruziunilor (IDSs) pot fi caracterizate și în funcție de sursa evenimentelor pe care le analizează. O clasificare clasică le împarte în sisteme IDS bazate pe date provenite de la un sistem, pe date provenite de la o aplicație specifică sau bazate pe date provenite din rețea.

5.4.1. Date specifice sistemului

Sistemele IDS care prelucrează date specifice sistemului (HIDSs) permit detectarea atacurilor care au ca țintă un calculator anume din rețea. Prin urmare, HIDSs analizează datele generate de către sistemul de operare al calculatorului gazdă. Aceste informații se mai numesc și date de audit și pot proveni din mai multe surse.

Sistemele de operare pun la dispoziția utilizatorului o serie de informații provenite direct din nucleul sistemului, privind procesele active, resursele de sistem utilizate, evenimentele de securitate relevante, prin intermediul câtorva utilitare foarte uzuale (de ex. *ps*, *netstat*, *top*, *vmstat*). Prin facilitatea de log-are Syslog, sistemul oferă posibilitatea înregistrării mesajelor generate de aplicațiile software pentru anumite evenimente. Totuși, informațiile generate sunt mai degrabă adaptate pentru procesul de depanare, și nu pentru necesitățile sistemelor IDS. Mai mult, nu există un format standard unic pentru informațiile înregistrate. Extragerea informațiilor pertinente din aceste log-uri devine astfel mai dificilă. Bineînțeles, în cazul unei intruziuni, mesajele înregistrate pot fi ușor modificate astfel încât urmele intruziunii să fie ascunse.

5.4.2. Date specifice aplicației

Sistemele IDS care prelucrează date specifice aplicației detectează atacurile împotriva unor aplicații. Informațiile utilizate pentru detecția intruziunilor sunt generate fie de mecanismul de log-are propriu al aplicației respective, fie de către mecanismul syslog al sistemului de operare.

Al doilea mecanism a fost prezentat în paragraful precedent. În ceea ce privește primul mecanism, este necesar ca aplicația software să permită generarea datelor de audit. Există mai multe soluții în acest scop:

- Prin modificarea directă a aplicației. Este posibilă doar pentru aplicațiile software în care avem acces la codul sursă;
- Prin interpunerea unui modul responsabil cu extracția informațiilor de audit, între aplicația respectivă și interfața de rețea utilizată. Acest modul poate intercepta apelurile funcțiilor de sistem, poate folosi biblioteci standard dedicate, etc. Un dezavantaj al acestei abordări îl constituie faptul că pot fi afectate și alte aplicații care rulează pe acel sistem, afectându-se astfel performanțele de operare;
- Prin extinderea aplicației. O serie de aplicații foarte flexibile oferă mecanisme de implementare a funcționalităților de audit.

5.4.3. Date specifice rețelei

Sistemele IDS care prelucrează date specifice rețelei (NIDSs), folosesc traficul de rețea captat pentru detectarea atacurilor.

Prin analiza conținutului pachetelor de date de rețea captate, se pot genera o serie de informații audit: caracteristici ale diferitelor antete și protocoale, număr de pachete, număr de conexiuni într-un interval, dimensiunea medie a pachetelor recepționate/transmise, număr de porturi utilizate, număr de adrese de rețea, etc.

Sistemele NIDSs sunt foarte întâlnite datorită ușurinței de instalare și a performanțelor lor. Totuși, trebuie avute în vedere și câteva limitări:

- rețelele de mare viteză pesupun un volum foarte mare al traficului de rețea, putând astfel provoca depășirea capacității de procesare a NIDSs;
- adoptarea criptării comunicațiilor din rețea reduce substanțial volumul informațiilor utile ce se pot extrage prin analiza conținutului pachetelor de date;
- o serie de analize recente au arătat vulnerabilitatea NIDSs la anumite atacuri

5.5. Tipuri de atacuri

O intruziune într-un calculator sau într-o rețea, constă în o serie de acțiuni cu scopul de a încălca politicile de securitate stabilite privind utilizarea corectă și legală a resurselor rețelei sau sistemului respectiv. Pentru dezvoltarea unor sisteme IDS performante și eficiente, este importantă cunoașterea cât mai bună a atacurilor existente și a tehnicilor utilizate în acest scop.

Aceste atacuri se pot împărți în cinci mari categorii, în funcție de acțiunile și scopul atacatorului [Haines99]:

- Atacuri de tip **Denial-of-Service** (DoS): au ca scop limitarea sau blocarea serviciilor oferite într-o rețea. Un exemplu des întâlnit, este atacul SYN-Flood, în care atacatorul bombardează sistemul țintă cu cereri de stabilire de conexiuni TCP, mult mai multe decât poate prelucra sistemul respectiv, sistemul neputând astfel să răspundă cererilor legitime.

- Atacuri de tip **Scan**: au ca scop strângerea de informații privind existența sau configurația sistemelor din rețea. Un exemplu comun de astfel de atac îl

reprezintă scanarea unei întregi clase de adrese IP pentru a identifica sistemele active din rețeaua respectivă.

- Atacuri de tip **Acces local-de-la-distanță**: sunt acele atacuri care încearcă nepermis, din exterior, să cîştige acces local la un calculator sau rețea (de ex. ghicirea unei parole a unui utilizator în vederea dobândirii accesului neautorizat în sistem).

- Atacuri de tip **Acces utilizator-administrator**: au ca scop dobândirea ilegală de către utilizatorii normali ai sistemului, a accesului privilegiat, de tip administrator. Există mai multe metode în acest sens: exploatarea vulnerabilităților de tip "buffer-overflow" a aplicațiilor sau sistemelor de operare, etc.

- Atacuri de tip **Data**: presupun accesul neautorizat prin diferite metode, la informații secrete sau confidențiale (de ex. fișiere, directoare, etc.).

În prezent, tot mai multe atacuri au evoluat, fiind proiectate în așa fel încât să nu poată fi detectate de către sistemele IDSs, ascunzând urmele lăsate în rețea sau în sistemul țintă. Există o serie de tehnici în acest scop: desfășurarea unui atac pe durata mai multor conexiuni de rețea; execuția întârziată a atacului; integrarea atacului în sesiuni ce apar ca și trafic normal; ascunderea comenzilor introduse în linia de comandă de către atacator, etc.

Atacuri de tip Denial-of-Service (DoS)

Atacul de tip DoS este definit ca și încercarea unui utilizator cu intenții malițioase, de a consuma resursele de calcul sau de memorie ale unui sistem dintr-o rețea, blocând astfel accesarea de către utilizatorii legitimi a serviciilor furnizate în rețeaua respectivă. Există o serie de metode în acest scop: inundarea cu un volum mare de trafic, pentru consumarea lățimii de bandă a rețelei, pentru umplerea memoriei tampon (buffer) a rutereilor, pentru acaparea totală a timpului de calcul al procesorului. În funcție de numărul de sisteme implicate în declanșarea atacului, atacurile DoS se împart în două mari categorii – atac singular, în care un singur sistem din rețea este responsabil cu generarea atacului, și atacul distribuit, în care mai multe sisteme se coordonează în lansarea atacului asupra țintei. Deoarece în atacurile DoS din cea de-a doua categorie sunt implicate mai mult decât un sistem din rețea, atacurile de acest tip sunt mai dificil de detectat.

În continuare sunt prezentate câteva din cele mai importante atacuri de tip DoS.

Atacul SYN Flood: Atacul exploatează mecanismul de funcționare al stivei de protocoale TCP/IP, mai exact al protocolului TCP (Transmission Control Protocol) orientat pe conexiune. O conexiune TCP între două sisteme este stabilită în trei pași. În prima etapă, sistemul sursă trimite o cerere SYN sistemului destinație. Apoi, sistemul destinație răspunde cererii printr-o confirmare SYN-ACK, alocând de asemenea o structură de date ce conține informații despre această conexiune care urmează a fi stabilită. În final, sistemul sursă răspunde și el printr-o confirmare, iar odată cu recepționarea acestei confirmări, sistemul destinație șterge structura de date memorată anterior, asociată conexiunii respective. Dacă în schimb un atacator, în prima etapă de stabilire a conexiunii folosește o adresă IP sursă contrafăcută, atunci ultima etapă nu mai este finalizată. În acest caz, informațiile despre conexiunea în curs sunt păstrate o perioadă de timp limitată, după care sunt șterse din memorie. Deoarece, fiecare sistem are limitări privind numărul maxim de conexiuni în așteptare, ce pot fi stocate la un moment dat în memorie, un atacator cu intenții malițioase poate să trimită un număr foarte mare de astfel de cereri SYN

cu adrese IP contrafăcute, astfel încât să umple zona de memorie rezervată stocării conexiunilor, sistemul atacat blocându-se, neputând satisface în continuare cererile de stabilire de noi conexiuni, legitime.

Atacul UDP Flood: Are ca efect încetinirea și congestionarea rețelei, precum și blocarea sistemului țintă. Atacul se realizează prin trimiterea unui volum mare de pachete de date, cu adresa IP sursă diferită de cea reală, la unul dintre porturile sistemului atacat. Sistemul țintă prelucrează aceste pachete, ca apoi să le șteargă constatând că nu sunt valide. Tot acest proces însă, consumă din timpul și puterea de prelucrare a procesorului, și datorită numărului mare de astfel de pachete, e posibil ca sistemul țintă să cedeze. În plus, deoarece protocolul UDP (User Datagram Protocol) nu dispune de funcția de control a congestiei, creșterea ratei de transmisie este inevitabilă, ducând în final la scăderea vitezei de transmisie în rețeaua respectivă.

Atacul Smurf: Atacul presupune trimiterea de pachete ICMP (Internet Control Message Protocol) "echo request", la adresele de difuzare (broadcast) a rețelelor vulnerabile. Aceste pachete au adresa IP sursă ca fiind adresa IP de rețea a sistemului care se dorește a fi atacat. În acest fel, fiecare sistem din rețeaua respectivă, răspunde cu un pachet ICMP de tip "echo reply" trimis sistemului victimă, generându-se un volum foarte mare de trafic în rețea și consumându-se lățime de bandă.

Atacul Ping of Death: Este un atac în care asupra sistemului țintă se trimit un număr mare de pachete de date de dimensiuni mai mari decât 65536 bytes, dimensiunea maximă permisă de protocolul IP. Are ca efect, necesitatea fragmentării acestor pachete, ceea ce duce la încărcarea procesorului și la consumul lățimii de bandă.

Atacul DNS Flood: În fiecare rețea din Internet există sisteme specializate ce oferă servicii de tip DNS (Domain Name Server), de obicei un server primar și/sau mai multe servere secundare. În mod constant, serverele secundare de DNS își actualizează informațiile DNS despre o anumită zonă prin cereri trimise serverului DNS central. Însă, dacă un atacator trimite astfel de cereri în mod repetat, datorită fluxului mare de date vehiculate, lățimea de bandă disponibilă scade foarte mult.

Atacul Mailbomb: Este un atac ce trimite un număr mare de mesaje email unui server din rețea, umplând coada de mesaje a serverului și suprasolicitând serviciul respectiv.

Atacul Apache2: Este un atac asupra aplicației de web server apache, în care un client trimite o cerere cu numeroase antete http. Pentru un număr mare de astfel de cereri, serverul va răspunde tot mai lent, putându-se chiar bloca în final.

Atacuri de tip Scan

În ultimii ani au fost dezvoltate tot mai multe aplicații care scanau automat o întreagă rețea de calculatoare cu scopul de a strânge informații și a identifica vulnerabilități cunoscute. Administratorii de sistem și rețea, persoanele responsabile cu securitatea folosesc astfel de aplicații de scanare a rețelelor în diferite scopuri: audit de securitate, testare, management, inventarierea sistemelor și a rețelei. De exemplu, scanarea care are ca scop identificarea serviciilor și a sistemului de operare este utilă în procesul de actualizare a aplicațiilor software. Scanarea porturilor, este utilă în verificarea porturilor deschise, astfel încât să corespundă cu politica de securitate stabilită, în timp ce scanarea rețelei este utilă în verificarea funcționării corecte a aplicațiilor firewall din rețeaua respectivă. Din nefericire,

aceste tipuri de aplicații pot fi foarte utile utilizatorilor cu intenții malițioase în identificarea posibilelor ținte înainte de a concepe un atac.

Scanarea unei rețele este procesul prin care se descoperă sistemele active din rețea și se obțin informații utile despre acestea, cum ar fi: sistemul de operare instalat, aplicațiile, serviciile și porturile active. Există mai multe tehnici de scanare: maparea rețelei, scanarea porturilor, detecția serviciilor și identificarea versiunii lor, detecția sistemului de operare. Aceste tehnici de scanare de bază pot fi "îmbunătățite" prin mascarea originii procesului de scanare, prin utilizarea sincronizării de timp cu scopul de a face invizibil procesul de scanare și a evitării aplicațiilor de apărare de tip firewall.

Descoperirea sistemelor active: Este primul pas în scanarea rețelelor. Presupune încercarea de a determina un sistem țintă să emită un răspuns, printr-o serie de tehnici:

- **ICMP Echo Request:** O cerere ICMP Echo este un pachet ICMP de tip 8, denumit în mod obișnuit ca și ping. Dacă adresa IP țintă este activă, acel sistem va genera un răspuns de tip ICMP Echo Reply (ICMP de tip 0). Trimiterea de astfel de pachete la mai multe adrese IP este cunoscută ca și ping sweep.

- **ICMP timestamp:** Este o cerere ICMP de tip 13, iar un sistem activ va răspunde cu un pachet ICMP de tip 14, ce reprezintă timpul curent al sistemului respectiv.

- **ICMP Address Mask request:** Reprezintă o cerere ICMP de tip 17, prin care se solicită masca adresei de rețea. Sistemul țintă activ va răspunde cu un pachet ICMP de tip 18.

- **TCP Ping:** Această tehnică presupune trimiterea unui pachet TCP SYN sau TCP ACK către o adresă IP țintă, la un port oarecare, specificat. Dacă sistemul vizat este activ va răspunde, cu un pachet în funcție de cererea primită, de versiunea sistemului de operare, de prezența unui firewall.

- **UDP Ping:** În acest caz, se trimite un pachet UDP către un port UDP specific. Dacă sistemul țintă este activ și portul respectiv deschis, sistemul nu va genera nici un fel de răspuns. Dacă însă, portul este închis sistemul va genera un răspuns de tip ICMP Port Unreachable (port ICMP inaccesibil).

Însă, aceste metode de detecție nu sunt în totalitate de încredere. Dacă un sistem nu generează nici un fel de răspuns, este posibil ca sistemul să fie totuși activ, pachetele fiind însă filtrate de către ruter sau firewall.

Scanarea porturilor și a serviciilor: După identificarea unui sistem activ într-o rețea, următorul pas al unui atacator îl reprezintă identificarea porturilor deschise și a serviciilor disponibile, cu scopul de a ajuta ulterior atacatorul să găsească vulnerabilități care să-i permită intruziunea neautorizată în sistemul respectiv. Există mai multe metode de scanare a porturilor:

- **Scanarea Connect:** Metoda realizează o conexiune TCP cu sistemul țintă. Dacă portul TCP scanat este deschis și nu este filtrat de către firewall, va răspunde cu un pachet de confirmare SYN/ACK, iar dacă este închis va genera un pachet RST/ACK. Această tehnică de scanare a porturilor este ușor detectabilă, acțiunea fiind înregistrată de către sistemul scanat.

- **Scanarea SYN:** Este cunoscută ca și o conexiune TCP "nefinalizată" (half-open), și a apărut cu scopul de a evita înregistrarea conexiunii TCP pe sistemul țintă. În momentul în care sistemul care inițiază conexiunea recepționează pachetul de confirmare SYN/ACK din partea sistemului scanat, acesta închide brusc conexiunea trimițând un pachet RST. Cu toate că acest tip de scanare nu este

înregistrat de către sistemul de operare al sistemului, este ușor detectabilă de către sistemele IDS.

- **Scanarea FIN:** Deoarece scanarea SYN este ușor detectabilă prin monitorizarea pachetelor SYN la porturile nepermise, o soluție pentru a evita detectarea scanării o reprezintă utilizarea pachetelor FIN. Ideea se bazează pe faptul că porturile închise răspund unui pachet FIN cu un pachet RST, în timp ce porturile deschise ignoră aceste pachete. Acest fapt reprezintă o eroare de implementare a stivei de protocoale TCP.

- **Scanarea FTP:** Această tehnică se folosește de caracteristica "FTP proxy" a unui server FTP (File Transfer Protocol) pentru a scana un sistem țintă. Această caracteristică "FTP proxy" permite unui utilizator să se conecteze la un server FTP și să solicite trimiterea unui fișier la un alt sistem. Astfel, prin acest proces se poate determina dacă un port este deschis sau nu. În plus, prin scanarea FTP se poate evita blocarea de către un firewall, deoarece scanarea se face de pe serverul FTP din rețeaua respectivă, care probabil nu este filtrat.

- **Scanarea XMAS:** Face parte din grupul de tehnici mai subtile de scanare. Scanarea XMAS determină porturile deschise prin trimiterea de pachete invalide, mai exact pachete cu câmpurile Finish (Fin), Push (PSH) și Urgent (URG) setate. Deoarece pachete cu o astfel de combinație nu există în traficul de rețea real, nu există nici un fel de regulă stabilită în ceea ce privește răspunsul la acest tip de pachete. Astfel, în unele implementări TCP, un port închis va răspunde cu un pachet RST/ACK iar un port deschis nu va genera nici un răspuns. În alte implementări TCP, se va genera ca răspuns un pachet RST indiferent dacă portul este deschis sau închis, în timp ce în alte implementări ale stivei TCP nu se va genera nici un fel de răspuns.

- **Scanarea NULL:** La fel ca și scanarea XMAS, această tehnică se bazează pe trimiterea unor pachete invalide. Scanarea NULL folosește pachete care nu au nici un câmp activat. Porturile închise vor răspunde cu un pachet RST/ACK, iar porturile deschise vor ignora aceste pachete. Alte sisteme vor genera în fiecare situație un pachet RST, sau nici un fel de răspuns.

- **Scanarea TCP Idle:** Această metodă ingenioasă permite scanarea complet invizibilă, prin utilizarea unui alt sistem, de pe care se face scanarea, denumit sistem zombie. Fiecare pachet IP transmis în Internet are un număr de identificare de fragmentare (IP ID). Deoarece majoritatea sistemelor incrementează acest număr pentru fiecare pachet transmis, prin sondarea numărului IP ID, este posibil de a determina numărul de pachete transmise între două operațiuni de sondare. O scanare de tip TCP Idle are trei pași: 1) atacatorul trimite un pachet SYN/ACK sistemului zombie care răspunde cu un pachet RST, dezvăluindu-și astfel numărul IP ID; 2) atacatorul generează un pachet SYN contrafăcut, ca fiind generat de către sistemul zombie, și îl trimite la un port de pe sistemul țintă. Dacă portul respectiv este deschis, sistemul țintă va trimite ca răspuns un pachet SYN sistemului zombie, care va genera la rândul lui un pachet RST, incrementându-și astfel numărul IP ID. Dacă însă, portul este închis, sistemul țintă trimite înapoi un pachet RST, sistemul zombie ignorând acest pachet, astfel numărul IP ID rămânând neschimbat; 3) atacatorul sondează din nou numărul IP ID al sistemului zombie, trimițând un pachet SYN/ACK. După acest proces, numărul IP ID s-a mărit fie cu una sau cu două unități. O creștere cu doi, indică faptul că portul este deschis iar o creștere cu unu, un port închis sau filtrat.

După descoperirea porturilor deschise, un atacator poate rula investigații suplimentare pentru identificarea versiunii serviciului ce rulează pe acele porturi de comunicare, identificate anterior.

Detecția sistemului de operare: Pentru un atacator este vitală informația privind tipul sistemului de operare ce rulează pe sistemul țintă. Identificarea sau "amprentarea" (fingerprinting) sistemului de operare se poate realiza în mod activ sau pasiv. Modul activ de scanare presupune trimiterea de pachete cu diferite caracteristici către sistemul țintă, și apoi analizarea răspunsurilor generate și compararea cu o listă cunoscută de perechi cerere/răspuns, pentru a găsi o potrivire. Acest mecanism se bazează pe modul de implementare a stivei de procoale TCP/IP precum și pe caracteristicile acestor protocoale (de ex. mărimea ferestrei TCP, numărul de secvență TCP, timpul de viață IP, codul de răspuns ICMP, suma de control UDP, etc.).

Mecanismul de scanare pasivă pentru identificarea sistemului de operare, este identic cu cel utilizat în metoda activă, doar că se bazează pe analiza traficului de rețea captat, prin urmare această metodă nu presupune trimiterea de pachete către sistemul scanat. Acest tip de scanare este mult mai dificil și complex deoarece trebuie analizat orice trafic din rețea, nefiind suficientă trimiterea de pachete de test, special concepute.

Majoritatea tehnicilor de scanare a rețelelor sunt ușor de detectat sau sunt filtrate de către aplicațiile firewall și routere. Prin urmare, atacatorii au apelat la diferite metode de scanare pentru evitarea detectării, cum ar fi:

Scanarea lentă – această tehnică limitează numărul de sisteme și porturi ce sunt scanate într-o perioadă de timp. Intervalul de timp, este însă foarte lung, cu scopul de a reduce probabilitatea de detecție. Deoarece majoritatea sistemelor IDS caută să identifice un număr mare de conexiuni într-un interval de timp relativ mic, o astfel de tehnică de scanare are mari șanse de a nu fi detectată.

Fragmentarea – presupune împărțirea cererilor TCP în mai multe pachete.

Ascunderea identității (address spoofing) – se realizează prin schimbarea adresei IP sursă reală a sistemului care efectuează scanarea. Această tehnică nu este însă utilă în cazul în care atacatorul dorește să recepționeze rezultatele scanării, pentru a obține informații despre sistemul țintă. În schimb este eficientă în evitarea unor măsuri de securitate a rețelelor, cum ar fi autentificarea pe bază de adresă IP. O posibilitate de a limita această tehnică, este prin filtrarea întregului trafic de ieșire, în dispozitivul de rețea care face rutarea dintr-o rețea în alta, astfel încât adresa sursă a pachetelor trimise să corespundă clasei de adrese a rețelei respective.

Porturile sursă – pe lângă ascunderea identității, o altă tehnică de evitare a aplicațiilor de tip firewall, este aceea de a schimba portul sursă al pachetelor ce sunt trimise în rețea cu un port care este acceptat de către aplicația firewall (de ex. portul 53 DNS).

Opțiunile IP – prin schimbarea opțiunilor protocolului IP se poate evita blocarea pachetelor de către aplicația firewall sau se pot specifica alte rute alternative către sistemul țintă.

Există un număr mare de aplicații de scanare a rețelelor, gratuite sau comerciale din care amintim: Nmap, Nessus, GFI LANguard, Hping2, Netcat, Superscan, Nikto, Satan, THC Amap, Scapy, Sam Spade, P0f, Nbtscan, WebInspect, Xprobe2, SolarWinds, Firewalk, Angry IP Scanner, Ike-scan, Nemesis, ISS Internet Scanner, SPIKE Proxy, Yersinia, X-scan, Whisker/libwhisker, Sara, QualysGuard, cheops/cheops-ng, Burpsuite, Unicornscan, Fping, Wikto, Scanrand, Canvas, Tcptraceroute, SAINT, Acunetix WVS, Rational AppScan, N-Stealth, MBSA, YAPS, NEWT.

Atacuri de tip Acces-local-de-la-distanță

Sunt atacuri în care un atacator dobândește accesul neautorizat de utilizator într-un sistem, prin exploatarea unor vulnerabilități existente în rețeaua sau sistemul respectiv. Vulnerabilitățile pot rezulta dintr-o serie variată de cauze: utilizarea de parole slabe care pot fi foarte ușor ghicite de către utilizatori cu intenții malițioase, vulnerabilități ale aplicațiilor software ("bugs"), viruși și programe "malware", injectarea de cod, configurări greșite ale serviciilor disponibile în Internet, manipularea utilizatorilor de a efectua acțiuni prin care să își dezvăluie informații sensibile ("social engineering"). Tipuri frecvente de defecte software ce conduc la apariția vulnerabilităților includ:

Coruperea de memorie – Supra-încărcarea memoriei tampon (buffer overflow) este o anomalie de funcționare a unui program, care în timp ce scrie date într-o zonă de memorie, depășește spațiul alocat, rescriind o zonă de memorie adiacentă. Are ca efect un comportament imprevizibil și necontrolat al programului respectiv, cum ar fi: erori de acces la memorie, rezultate incorecte, terminarea bruscă a programului sau compromiterea securității sistemului. Un alt tip de defect îl reprezintă utilizarea pointer-ilor invalizi, care nu indică către nici un obiect valid din memorie. Acești pointer-i apar când un obiect este șters sau dealocat din memorie, fără însă a modifica și valoarea pointer-ului corespunzător, astfel pointer-ul indică în continuare către acea zonă din memorie ce a fost dealocată. Efectul asupra comportamentului produsului software este același ca și în cazul defectelor de tip "buffer overflow". Numeroase aplicații server de rețea prezintă astfel de vulnerabilități: imap, named, sendmail, etc.

Erori de validare a intrărilor – Se pot clasifica în: erori de formatare a șirurilor de caractere – problema provine din neverificarea datelor de intrare din funcțiile de citire/scriere, fiind astfel posibilă forțarea unui program de a rescrie adresa din memorie a funcției respective sau adresa returnată din stiva de memorie, cu un pointer ce indică o bucată de cod malițios; injectarea SQL – este o tehnică de injectare de cod malițios, ce exploatează vulnerabilități de securitate din operațiile cu o bază de date, mai exact se datorează lipsei de filtrare a caracterelor "escape" (caractere ce determină o interpretare alternativă a caracterelor ulterioare) din datele introduse de utilizator, ce urmează a fi folosite într-o interogare SQL, putându-se astfel manipula interogările efectuate în baza de date; injectarea E-mail – este posibilă în aplicațiile Internet folosite pentru transmiterea de mesaje email, prin exploatarea malițioasă a formatului MIME (Multipurpose Internet Mail Extensions) prin care se pot adăuga informații suplimentare mesajului ce urmează a fi trimis, cum ar fi o nouă listă de destinatari sau un nou conținut al mesajului. Trimiterea unui număr mare de astfel de mesaje email nesolicitate este cunoscută și sub denumirea de "spamming"; injectarea paginilor web – cunoscută sub denumirea de "cross-site scripting" (XSS), presupune injectarea unor script-uri în partea de client a unor pagini web, vizualizate de un alt utilizator. Prin astfel de atacuri, un atacator poate obține accesul privilegiat la unele pagini cu conținut sensibil sau la o serie de alte informații menținute de către aplicația de vizualizare a paginilor web ("browser") pentru utilizatorul respectiv. În ultimii ani, acest tip de vulnerabilitate a depășit ca număr vulnerabilitățile de tip buffer overflow, devenind vulnerabilitatea de securitate cel mai des raportată.

Condiții de concurență – Acestea pot apărea în aplicațiile software, atunci când mai multe procese sau fire de execuție accesează o resursă comună, prin execuția unei bucăți de cod numită secțiune critică. Operațiile asupra resursei comune trebuie să se excludă reciproc, pentru a evita coliziunile dintre diferitele

procese care împart aceeași resursă de sistem. Accesul concurențial poate fi evitat prin impunerea unui mecanism de sincronizare, ce controlează execuția secțiunii critice.

Escaladarea privilegiilor – Are loc atunci când o aplicație software are un defect care permite ocolirea verificărilor de securitate și permite, accesul la resurse care în mod normal ar fi fost protejate față de aplicația respectivă. Rezultă astfel, un comportament nedorit al aplicației, prin dobândirea unui nivel de acces mai ridicat la resursele sistemului.

Atacuri de tip Acces-utilizator-administrator

Aceste atacuri au ca scop dobândirea accesului privilegiat, de tip administrator, al unui utilizator normal al sistemului. Compromiterea utilizatorului de tip administrator, de către un atacator este echivalentă cu compromiterea definitivă a sistemului atacat, în cele mai multe cazuri necesitând reinstalarea completă a sistemului, cu un sistem de operare și aplicații actualizate. Ca și atacurile de tip acces-local-de-la-distanță, atacurile de tip access-utilizator-administrator au la bază exploatarea vulnerabilităților existente în aplicațiile software sau în sistemul de operare. Aceste probleme au fost prezentate în paragraful anterior.

5.6. Considerații privind îmbunătățirea performanțelor IDSs

Deși în ultimii 20 de ani s-au înregistrat nenumărate progrese în domeniul detecției intruziunilor, au rămas o serie de probleme ce nu au fost rezolvate sau pot fi îmbunătățite. Provoacă sunt numeroase: dezvoltarea rapidă a tehnologiilor (de ex. rețelele mobile și wireless), creșterea vitezei rețelelor, criptarea comunicațiilor, etc. Prin urmare, modelele noilor sisteme IDS trebuie să răspundă acestor schimbări permanente a dispozitivelor și tehnologiilor de rețea.

Problema colectării celor mai relevante informații este foarte importantă. Detecția exactă a unui atac presupune analiza unor date complete și de încredere privind activitatea sistemului supravegheat de către IDS. Majoritatea sistemelor de operare dispun de mecanisme de înregistrare a activităților efectuate de către utilizatori sau de către aplicații, cum ar fi: tentativele eșuate de autentificare, apelurile funcțiilor de sistem de către procesele active, inițierea conexiunilor de rețea, captarea pachetelor din rețea. Cu cât informațiile de audit sunt mai detaliate și complete, cu atât necesitățile de prelucrare și de stocare sunt mai mari, ceea ce poate duce la scăderea performanțelor sistemelor IDSs. De exemplu, captarea totală a traficului de rețea într-o rețea de bandă largă, poate necesita sute de GB pe zi. În consecință, este important de a decide ce informații sunt relevante pentru diferitele tipuri de atacuri întâlnite în practică. Suntem astfel în fața unui compromis privind volumul informațiilor captate de către IDS, între gradul de încărcare al sistemului și eficacitatea lui.

O problemă continuă a sistemelor IDSs bazate pe detecția anomaliilor o constituie numărul relativ mare de alerte false. Astfel, probabilitatea ca sistemul IDS să se blocheze din cauza generării unui număr foarte mare de alarme false, este foarte ridicată. În plus, numărul de alerte false trebuie să fie foarte mic în raport cu numărul de evenimente malițioase, pentru ca sistemul IDS să fie eficient. Prin urmare, una din prioritățile de cercetare în dezvoltarea noilor generații de sisteme

IDSs, o constituie rezolvarea acestei probleme, de minimizare a ratei de alarme false.

Modelarea datelor, mai exact utilizarea unor date de evaluare care să simuleze cât mai real atacurile existente în realitate, reprezintă o altă temă stringentă în detecția anomaliilor. De exemplu, foarte multe dintre sistemele IDSs propuse, sunt evaluate cu setul de date furnizat de către DARPA/MIT Lincoln [DARPA99], KDDCup 1999 Data [KDD99]. Deși aceste date de evaluare sunt foarte utile în testarea și antrenarea sistemelor IDS, o serie de cercetări [Hugh00], au arătat faptul că metodele folosite pentru generarea datelor de test, nu sunt tocmai potrivite în simularea atacurilor întâlnite în realitate.

O altă problemă legată de sistemele IDS ce analizează traficul de rețea captat, o reprezintă utilizarea pe scară largă a criptării comunicațiilor în rețea (de ex. rețelele VPN – Virtual Private Network, IPsec – Internet Protocol Security, SSL – Secure Socket Layer, SSH – Secure Shell, etc.). În acest caz, informațiile necesare detecției intruziunilor, se obțin doar din analiza antetelor pachetelor captate, limitând astfel posibilitatea de detecție a unor clase de atacuri, de către sistemele IDS ce presupun analiza conținutului pachetelor captate, și nu doar a antetelor lor.

De asemenea, este foarte importantă stabilirea noțiunii de “normal” în ceea ce privește anumite caracteristici ale unei rețele, în absența atacurilor: volumul traficului, număr de conexiuni, dimensiunea medie a pachetelor, porturile accesate, corelarea adreselor IP, etc. Pentru stabilirea acestor caracteristici de referință, este necesară o înțelegere mult mai riguroasă a anomaliilor specifice rețelelor sau sistemelor, precum și înțelegerea tehniciilor utilizate în atacurile informatice.

Un aspect destul de delicat, neglijat în bună măsură [Axel98], care trebuie avut în vedere în proiectarea sistemelor IDS, este capacitatea de auto-apărare a sistemelor IDS împotriva atacurilor. Pentru a determina sistemul IDS să genereze necontrolat nenumărate alerte, cu scopul de a bloca în final sistemul respectiv, un atacator poată să trimită pachete de date special generate astfel încât să nu constituie un atac în sine, dar să determine aplicația IDS să le considere posibile intruziuni. Datorită acestei slăbiciuni persistente, este necesară o îmbunătățire a securității aplicației IDSs.

Un potențial mare de amenințări într-o rețea îl constituie atacurile din interior. Aceste tipuri de atacuri sunt foarte greu de detectat, datorită dificultății de a stabili regulile de bază în ceea ce privește atacurile sau anomaliile din rețea și a multitudinii de profile de acces în rețea. Prin urmare, o direcție a cercetării trebuie îndreptată pentru găsirea unor soluții practice în acest sens.

Pe lângă procesul de colectare și analiză a informațiilor necesare detecției atacurilor, răspunsul unui sistem IDS la identificarea unui atac este la fel de important. Răspunsul unui sistem IDS poate lua diferite forme: generarea unei alerte, blocarea IP-ului atacatorului sau luarea unei măsuri și mai drastice, sub forma unui contra-atac. O atenție sporită trebuie acordată cazului unei contra-măsuri agresive, deoarece ea poate fi luată împotriva unei victime inocente: un atacator poate genera trafic de rețea, care pare să provină de la o anumită adresă, dar care este de fapt generat în altă parte. O soluție ar fi luarea unor decizii în funcție de gravitatea consecințelor atacului respectiv.

5.7. Utilizarea analizei wavelet în detecția anomaliilor

Constituindu-se drept o nouă tehnologie, detecția anomaliilor în traficul de rețea bazată pe analiza wavelet, a găsit în ultimii ani tot mai multe aplicații practice

în domeniul securității rețelelor. Localizarea foarte bună, atât în domeniul timp cât și în domeniul frecvență (o rezoluție bună în frecvență pentru frecvențe joase și o rezoluție bună în timp pentru frecvențe înalte), recomandă utilizarea "undișoarelor" în detecția iregularităților traficului de rețea. Într-adevăr, s-a observat că traficul de rețea real este foarte nestaționar, prezentând variații foarte bruște.

O serie de metode de detecție a anomaliilor din traficul de rețea au fost propuse până în momentul de față. În aceste studii, analiza wavelet presupune prelucrarea unor semnale care scot în evidență unele trăsături ale traficului de rețea cum ar fi: număr de fluxuri, număr de pachete, număr de octeți, etc. Mărimile statistice considerate, în algoritmi de decizie a intruziunilor, sunt de asemenea diverse: varianța, media, corelația, energia, entropia, deviația standard și medie, etc. Pentru evaluarea performanțelor diferitelor sisteme propuse, au fost utilizate fie date de trafic reale, captate din diferite rețele, fie date de trafic obținute prin simularea unor atacuri. În continuare, sunt prezentate câteva dintre tehnicile propuse în literatura de specialitate.

În [Barford02], autorii prezintă o metodă de detecție a anomaliilor din traficul de rețea bazată pe transformarea wavelet de tip "framelet", implementată cu filtre pseudo-spline. Datele utilizate în analizele efectuate, au fost obținute prin prelucrarea a două tipuri de date: pachete SNMP (Simple Network Management Protocol) și fluxuri de pachete IP, colectate de pe un router dintr-un campus universitar. Acestea sunt apoi transformate în diferite serii de timp: număr de fluxuri, număr de pachete, număr de octeți, mărimea medie a pachetelor, cu ajutorul unor utilitare software. Prin sinteza coeficienților wavelet, se propune formarea a trei semnale distincte, ce reprezintă componenta din semnal de frecvență joasă, medie și înaltă. Mai exact, componenta de frecvență joasă expune iregularitățile de lungă durată (mai multe zile), cea de frecvență medie captează variațiile zilnice din trafic iar componenta de înaltă frecvență corespund variațiilor rapide, de scurtă durată. Algoritm de detecție a iregularităților din traficul de rețea analizat, presupune următoarele etape: calculul variației semnalelor de frecvență medie și înaltă, cu câte o fereastră alunecătoare; combinarea celor două variații obținute anterior printr-o sumă ponderată; aplicarea unui prag pentru a decide asupra existenței anomaliilor de trafic. Conform rezultatelor prezentate de autori, cu această metodă se pot detecta cu succes, unele anomalii de scurtă și de lungă durată. Componenta de joasă frecvență, capabilă să identifice atacurile de lungă durată, nu este luată în considerare, cu toate că în realitate există și alte forme de atacuri ce corespund acestui tip de model. În plus, toată această analiză este făcută doar "postmortem".

Focalizându-se asupra unor tipuri specifice de atacuri în rețea, Ramanarran prezintă în [Raman02], o abordare numită WADeS (Wavelet-based Attack Detection Signatures) pentru detecția atacurilor DoS distribuite. Transformarea wavelet este aplicată semnalelor de trafic - utilizând un sistem de filtrare LRU (Least Recently Used) al fluxurilor de date, se determină numărul de octeți al traficului global - iar mecanismul pentru detecția atacurilor se bazează pe varianța coeficienților wavelet. Pragurile de decizie privind detecția atacurilor sunt determinate euristic, prin studiul traficului de rețea.

O altă metodă de detecție a anomaliilor, bazată pe analiza corelației adreselor IP de destinație și a numerelor de port, din traficul global de ieșire al unui router, prin prelucrarea antetelor pachetelor de date, atât în timp real cât și "postmortem", este prezentată în [Kim05]. Studiul pleacă de la ipoteza că adresele IP de destinație ale pachetelor vehiculate dintr-o rețea vor avea un grad ridicat de corelare, din mai multe motive: o mare parte din trafic este realizat din accesarea

site-urilor mai des vizitate; fiecare utilizator în parte, obișnuiește să acceseze aceleași site-uri web de-a lungul timpului; fluxurile de date de durată mare (de ex. descărcarea de fișiere, de conținut multimedia, etc.) tind să coreleze adresele IP la scări de timp mai mari. Astfel, un atac de tip DoS asupra unui singur sistem va avea ca efect creșterea corelației adreselor IP, în timp ce un atac aleator de tip "vierme" asupra mai multor sisteme, va avea ca efect scăderea corelației. Prin urmare, orice schimbare bruscă a semnalului de corelație poate fi folosită pentru detecția anomaliilor din trafic. Acest semnal de corelație este transformat prin aplicarea DWT, iar detecția finală, presupune compararea mărimilor statistice obținute (deviația standard și medie) cu niște praguri rezultate din analiza traficului.

În [Huang06] autorii au implementat o platformă de dezvoltare numită Waveman, de analiză wavelet a traficului de rețea în timp real. Prin contorizarea numărului de pachete și de octeți (odată la 5 secunde), a traficului captat cu ajutorul bibliotecii libpcap, se obțin semnalele inițiale. Analiza wavelet a acestor semnale de trafic, este făcută utilizându-se o fereastră cu o dimensiune de 5 minute (60 eșantioane). Pentru evaluarea performanțelor diferitelor funcții wavelet utilizate pentru detecție, au fost considerate două mărimi: deviația medie procentuală și entropia. În urma evaluării rezultatelor, s-a constatat ca funcțiile wavelet Coiflet și Paul, furnizează performanțe mai bune în detecția atacurilor considerate, de tip DoS și Scan.

Un sistem automat de detecție a atacurilor DoS este propus în [Dainotti06]. Arhitectura sistemului cuprinde două module distincte de analiză, unul bazat pe tehnici tradiționale de prelucrare de semnal, cum ar fi filtrarea adaptivă și suma cumulativă, și unul bazat pe transformarea wavelet continuă (CWT). În evaluarea performanțelor acestei abordări, o atenție deosebită este acordată estimării cât mai precise a intervalului de timp în care are loc atacul, precum și puterii de rezoluție în separarea atacurilor succesive.

Pentru a rezolva unele limitări ale detecției anomaliilor bazate pe analiza multi-rezoluție, legate de sensibilitate, rezoluție, complexitate de calcul, fereastra temporală de detecție utilizată, în [Chang06] este introdusă o nouă tehnică de detecție, care utilizează transformata wavelet de pachete (WPT). Metoda propusă, permite o descompunere adaptivă, îmbunătățindu-se astfel capacitatea de detecție a anomaliilor de frecvență mare și medie. Acest deziderat, se realizează prin reconstrucția selectivă a coeficienților wavelet din diferite niveluri de descompunere, și prin utilizarea unui algoritm de detecție statistic, ce are la bază un mecanism adaptiv de selecție a ferestrei temporale, în funcție de frecvența centrală wavelet (această frecvență diferă în funcție de nivelul de descompunere și de scările de timp. Algoritmul de detecție statistic are la bază, un sistem modificat al celui propus în [Barford02], considerându-se două ferestre de detecție pentru calcularea mărimilor statistice, varianța respectiv media coeficienților wavelet.

În [Wei09], cei doi autori prezintă o tehnică nouă de modelare a semnalelor de trafic pentru detectarea anomaliilor din rețea, ce combină teoria de aproximare wavelet și teoria de identificare a sistemelor. Pentru a descrie cât mai complet trăsăturile traficului de rețea, sunt definite și generate o serie de semnale caracteristice, utilizate ca semnale de intrare pentru sistemul propus. Pe baza acestora, este modelat traficul zilnic normal și reprezentat printr-un set de coeficienți wavelet de aproximare (se utilizează transformata DWT), care pot fi estimați folosind modelul ARX (AutoRegressive with eXogenous) de predicție. Acest model este utilizat în continuare pentru analiza semnalelor de trafic, după predicție obținându-se semnalul rezidual. În final, pentru identificarea vârfurilor din semnalul rezidual (care reprezintă anomaliilor din trafic), este implementat un algoritm bazat

pe modelul GMM (Gaussian Mixture Model). Rezultatele obținute arată o rată de detecție foarte bună în identificarea atacurilor și a duratei lor.

5.8. Arhitectura generală a sistemului de detecție

Arhitectura generală a sistemului IDS, pe care l-am propus în [Salagean10] și [SF10] este prezentată în figura 5.1, și conține următoarele componente centrale: Analiză trafic, Analiză Wavelet, Analiză statistică (Cum4) și Detecție anomalii.

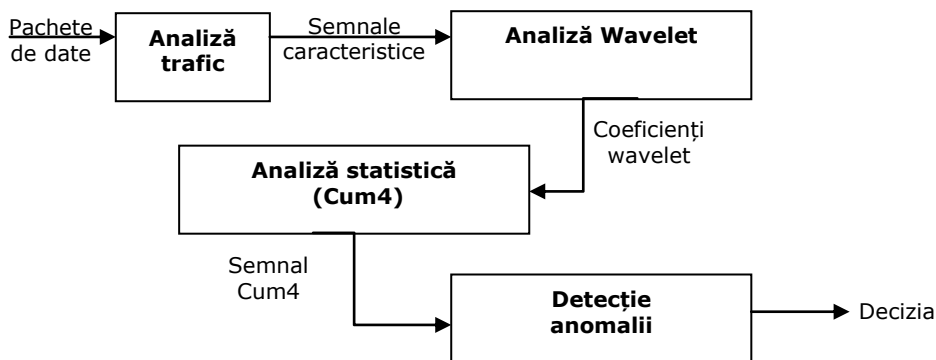


Figura 5.1. Arhitectura generală sistemului de detecție a anomaliilor

Blocul de analiză a traficului, are rolul de a capta traficul de rețea și de a genera un set de semnale caracteristice, definite astfel încât să descrie cât mai eficient trăsăturile traficului. Cu cât numărul de semnale caracteristice este mai mare, cu atât mai complete și pertinente vor fi informațiile privind volumul traficului dintr-o rețea, fiind posibilă astfel îmbunătățirea performanțelor de discriminare a comportamentelor anormale față de activitățile normale, obișnuite. Semnalele caracteristice sunt apoi transformate în coeficienți de aproximare și coeficienți de detaliu, cu ajutorul transformatei wavelet staționară și analitică (ASWT). Algoritmul statistic de detecție este aplicat coeficienților wavelet de detaliu de pe fiecare scară, utilizându-se o fereastră. Mărimea considerată pentru discriminare este valoarea locală (din fereastra alunecătoare) a cumulantului de ordin patru (Cum4), care face parte din categoria mărimilor statistice de ordin superior. Decizia privind detecția unei anomalii în semnalul de trafic analizat se face prin compararea valorii locale a cumulantului, cu niște praguri de decizie.

Toate aceste componente ale sistemului IDS propus, sunt prezentate în detaliu în paragrafele care urmează.

5.8.1. Analiza traficului de rețea

Așa cum am scos în evidență în paragraful precedent, rolul de bază al blocului de analiză a traficului, din arhitectura generală a sistemului de detecție, este acela de a caracteriza cât mai complet posibil, trăsăturile specifice ale traficului de rețea.

Traficul de rețea, captat în format *tcpdump* [Tcpdump], este transformat în primă fază în fluxuri de date. Un astfel de flux, în rețelele comutate de pachete,

reprezintă o secvență de pachete care circulă de la o anumită sursă la o destinație oarecare, într-un interval de timp. Mai exact, un flux de date TCP/IP, este unic determinat de următorii parametri: adresa IP sursă și destinație, portul sursă și destinație, protocolul IP. În prezent, majoritatea sistemelor de detecție a anomaliilor din trafic, utilizează aceste fluxuri de date.

În figura 5.2 este prezentată schema detaliată a blocului de analiză a traficului:

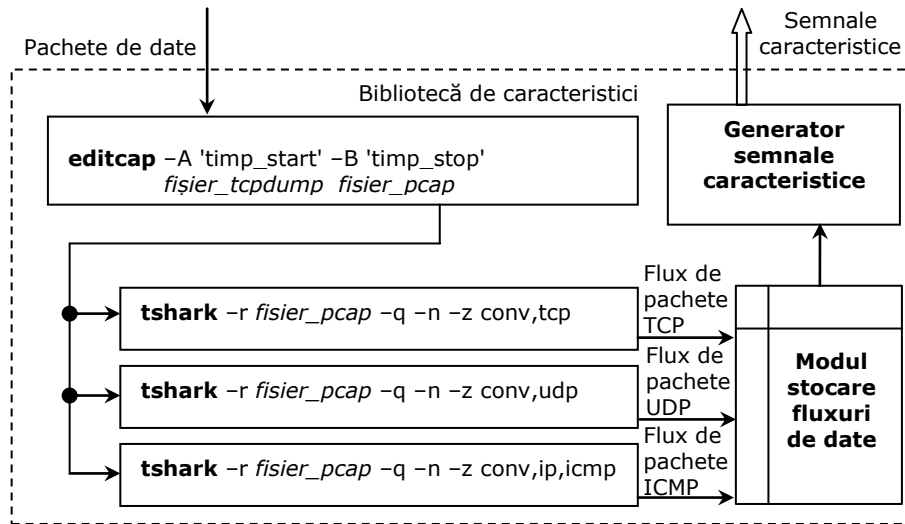


Figura 5.2. Blocul de analiză a traficului de rețea

Pachetele de date care sunt captate sub forma unor fișiere *tcpdump*, sunt convertite în fluxuri de pachete cu ajutorul a două utilitare de prelucrare a pachetelor salvate în format *libpcap*: *editcap* și *tshark*. Mai întâi, cu *editcap* se împarte fișierul original (*fișier_tcpdump*, în schema de mai sus) în mai multe fișiere cu extensia *pcap*, ce conțin doar pachetele care au fost captate între cele două momente de timp, *timp_start* și *timp_stop*, a căror format este *AAAA-LL-ZZ OO:MM:SS*. Diferența dintre aceste două mărimi, determină intervalul de eșantionare pentru semnalele caracteristice rezultate în final la ieșirea blocului de analiză a traficului.

În continuare, fluxurile de pachete de date sunt obținute via *tshark*, un utilitar de analiză a protocoalelor de rețea. Pentru fiecare din aceste fluxuri de pachete, se obțin următoarele informații: adresa IP sursă, portul sursă, adresa IP destinație, portul destinație, numărul de pachete primite, numărul de octeți primiți, numărul de pachete trimise, numărul de octeți trimiși, numărul total de pachete și numărul total de octeți. Protocoalele pachetelor din trafic considerate, sunt protocoalele TCP, UDP și ICMP.

Modulul de stocare a fluxurilor de date, are rolul de a salva într-o bază de date *MySQL*, pentru fiecare flux identificat, informațiile mai sus menționate, în vederea generării semnalelor de timp, definite conform unei biblioteci de caracteristici. Structura tabelului din baza de date are configurația următoare:

- flowId – identificatorul fluxului de date
- flowTimestamp – data de timp a fluxului de date

- srcIp – IP-ul sursă
- srcPort – portul sursă
- dstIp – IP-ul destinație
- dstPort – portul destinație
- inPackets – numărul total de pachete recepționate
- inFrames - numărul total de octeți recepționați
- outPackets - numărul total de pachete transmise
- outFrames - numărul total de octeți transmiși
- protocol – tipul protocolului pachetelor

De menționat că, intervalul de timp, pe durata căruia se determină fluxurile de pachete, este de o secundă, decizie luată din considerente de flexibilitate: din datele stocate în baza de date, se pot obține foarte ușor semnalele caracteristice cu un interval de eșantionare mai mare. O altă observație, este legată de faptul că în tabela din baza de date, nu sunt salvate informațiile privind numărul total de pachete și de octeți, deoarece această informație este redundantă (se poate determina din suma dintre numărul de pachete/octeți primiți și numărul de pachete/octeți trimise).

Mărimile care sunt utilizate în final pentru generarea semnalelor caracteristice, sunt prezentate în tabelul 5.1.

M_1, M_2, M_3	Număr de fluxuri (TCP, UDP, ICMP), într-un interval de timp
M_4, M_5, M_6	Număr mediu de pachete într-un flux (TCP, UDP, ICMP), într-un interval de timp
M_7, M_8, M_9	Număr mediu de octeți într-un flux (TCP, UDP, ICMP), într-un interval de timp
M_{10}, M_{11}, M_{12}	Număr mediu de octeți într-un pachet (TCP, UDP, ICMP), într-un interval de timp
M_{13}, M_{14}, M_{15}	Raportul dintre numărul de fluxuri și numărul mediu de octeți într-un pachet (TCP, UDP, ICMP), într-un interval de timp

Tabel 5.1. Mărimi caracteristice ale traficului de rețea

5.8.2. Analiza Wavelet

Transformarea DWT standard, așa cum am văzut în paragraful 1.2.2, permite o reprezentare compactă și neredundantă a semnalului în domeniul de transformare. Însă, datorită procedurii de decimare de după etapa de filtrare folosită în calculul transformatei, DWT este variantă la translațiile de timp. Aceasta constituie un mare dezavantaj în aplicațiile de prelucrare statistică a semnalelor, de exemplu, detectarea și estimarea parametrilor semnalului.

Pentru a rezolva acest dezavantaj, au fost introduse numeroase soluții. Una dintre aceste soluții o constituie transformarea wavelet staționară (SWT). În literatura de specialitate este cunoscută sub diferite nume cum ar fi: transformarea wavelet redundantă, ne-decimată, supra-completă sau invariantă la translații. Structura de implementare a SWT este similară cu cea a DWT, însă fără procedura de decimare (sub-eșantionare). Algoritmii de implementare este cunoscut ca și algoritmul "à trous", care modifică filtrele prin introducerea de zerouri [Mal99]. La ieșirea SWT, pentru fiecare nivel de descompunere se obține același număr de coeficienți, egal cu numărul de eșantioane din semnalul de intrare. Prin urmare, redundanța este de 2^J , unde J reprezintă numărul de iterații. Din considerente

practice, acest număr de iterații este limitat la valoarea $J = \log_2 N$, unde N este numărul de eșantioane al semnalului de intrare. Implementarea SWT este ilustrată în figura 5.3, unde $h[n]$ este răspunsul la impuls al filtrului trece-sus iar $g[n]$ este răspunsul la impuls al filtrului trece-jos. Operatorul $*$ reprezintă convoluția în timp discret.

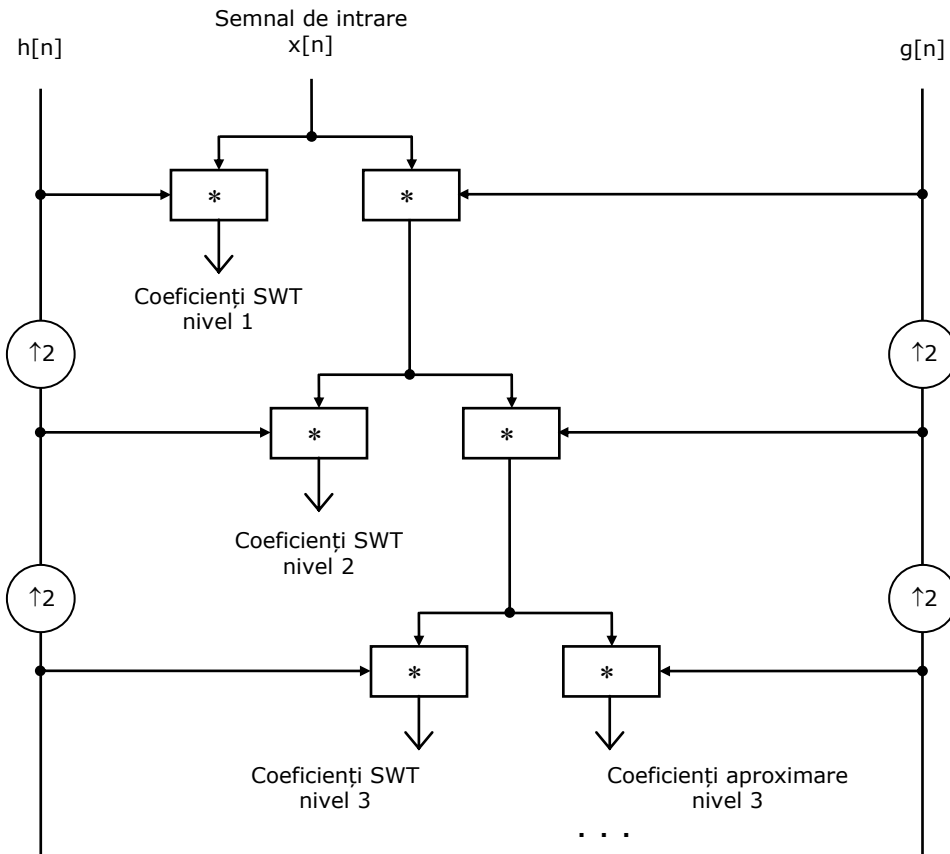


Figura 5.3. Implementarea SWT folosind bancuri de filtre

Implementarea SWT considerată în schema propusă în figura 5.1, este cea introdusă în [AOB06], [FIB09] pentru DWT. Transformarea rezultată astfel, este transformarea wavelet staționară analitică (ASWT). Aceasta este o transformare complexă, fiind aplicată semnalului analitic asociat semnalului de intrare. Semnalul analitic pentru un semnal $x(t)$, este definit în relația 5.1:

$$x_a(t) = x(t) + jH(x(t)) \quad (5.1)$$

Calculul ASWT presupune o singură operație SWT, folosindu-se undișoare mamă clasice (de ex. din familia Daubechies, Coiflet, etc.). Unul dintre dezavantajele undișoarelor mamă clasice este lipsa de simetrie a formei lor de undă. Din acest motiv caracteristicile lor de fază nu sunt liniare. Acest dezavantaj poate fi diminuat folosind undișoarele mamă analitice care apar folosind schema din figura

5.4. Undișoarele mamă analitice echivalente sunt funcții complexe având modulul mai simetric decât undișoarele mamă din care au fost construite. În figura 5.4 este ilustrată această implementare a ASWT:

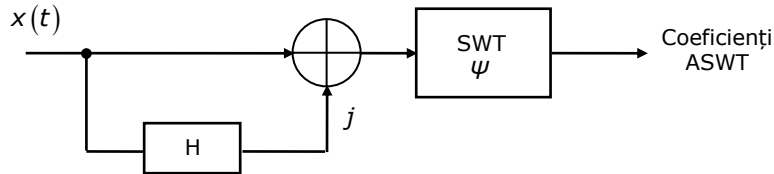


Figura 5.4. Implementarea ASWT

Prin aplicarea transformării ASWT rezultă coeficienții wavelet de aproximare și detaliu. Transformarea ASWT identifică schimbările din semnal pe diferite scări de timp. Astfel, pentru un interval de eșantionare $T_s=1$ minut, eșantioanele de pe nivelul j vor fi distanțate în timp cu $T_s \cdot 2^j$ minute.

5.8.3. Analiza statistică (Cum4) și detecția

Majoritatea sistemelor IDS bazate pe analiză wavelet pentru detecția anomaliilor de trafic utilizează ca și mărime statistică varianța locală. Calcularea varianței locale presupune utilizarea unei ferestre de detecție, glisantă în timp. Însă, aceste metode prezintă unele dezavantaje. În continuare, vom analiza un exemplu care să evidențieze aceste limitări. Considerăm un semnal de trafic, cu un interval de timp de eșantionare de un minut, care conține două anomalii: în momentul de timp $t = 200$, o anomalie cu amplitudine mare cu durata de 1 minut, și o altă anomalie cu o amplitudine mult mai mică, pe durata a 2 eșantioane, localizată în momentele de timp $t = 400$ și $t = 401$. Acest semnal de trafic este ilustrat în figura 5.5.

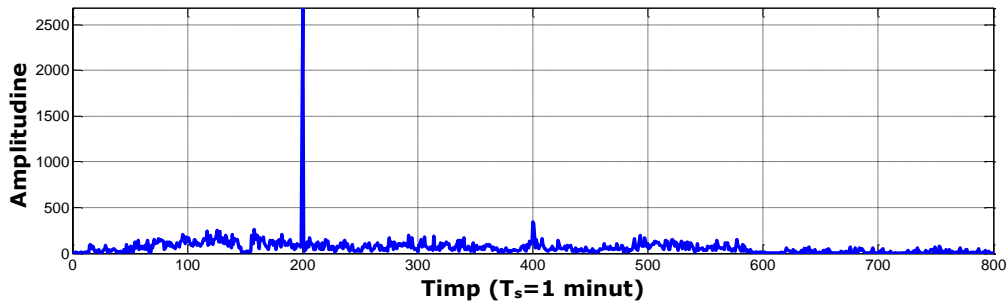


Figura 5.5. Semnal de trafic care conține 2 anomalii în $t=200$ și $t=400,401$

Pentru detecția atacurilor, semnalul de trafic din figura anterioară este prelucrat conform metodei propuse în figura 5.1. Algoritmul statistic este bazat pe calcularea varianței coeficienților wavelet. Semnalul de varianță a coeficienților wavelet (VWC) rezultat astfel este prezentat în figura 5.6.

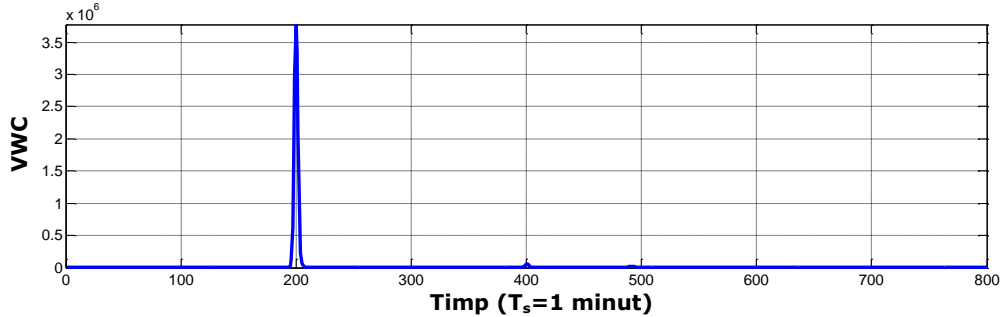


Figura 5.6. Semnalul VWC rezultat pentru semnalul de trafic din figura 5.5

Analizând rezultatele obținute în figura 5.6, se observă că în momentul de timp $t = 200$ se obține o valoare a varianței coeficienților wavelet (VWC) de $3,7 \cdot 10^6$ iar pentru $t = 400$ o valoare de $5,7 \cdot 10^4$. Datorită valorii prea mari a mărimii VWC obținute pentru prima anomalie, cea de-a doua anomalie poate trece neobservată, valoarea VWC, prin comparație, fiind extrem de mică. În aceste situații, alegerea pragului de decizie este mult mai critică, deoarece un prag puțin mai mare poate determina nedetectarea celei de-a doua anomalii. În plus, în urma simulărilor am constatat o dependență foarte mare a performanțelor de detecție a anomaliilor în funcție de lungimea fereastră de detecție considerată: o lungime prea mică determină scăderea performanțelor de detecție a anomaliilor.

Pentru a rezolva aceste dezavantaje, propunem utilizarea în algoritmul statistic de detecție a mărimilor statistice de ordin ridicat, mai exact, a cumulanzului de ordinul patru (Cum4). Cum 4 prezintă câteva proprietăți foarte importante: pentru semnale gaussiene este nul, valoarea sa fiind cu atât mai mare cu cât distribuția semnalului este mai diferită de o gaussiană. Prin urmare, dacă în fereastra de detecție, traficul prezintă anomalii, atunci valoarea cum4 va crește. Aceste caracteristici îl fac extrem de util în contextul analizei traficului de rețea, având în vedere caracterul puternic nestaționar al acestuia [Barford02].

Pentru p și q , se definește cu M_p^q , momentul complex a lui s în (5.2) și \tilde{M}_p^q estimarea sa, în (5.3).

$$M_p^q[s] = E(s^p s^{*q}) \quad (5.2)$$

$$\tilde{M}_p^q[s] = \frac{1}{N} \sum_{k=1}^{N-1} s^p(k) s^{*q}(k) \quad (5.3)$$

Cumulanzul de ordinul patru, \tilde{C}_2^2 este calculat cu:

$$\tilde{C}_2^2[s] = \tilde{M}_2^2[s] - 2(\tilde{M}_1^1[s])^2 - \tilde{M}_2[s]\tilde{M}^2[s] \quad (5.4)$$

În figura 5.7 este redat semnalul Cum4 (CWC), obținut pentru semnalul de trafic de test din figura 5.5. Parametrii de simulare sunt identici cu cei folosiți pentru obținerea semnalului VWC.

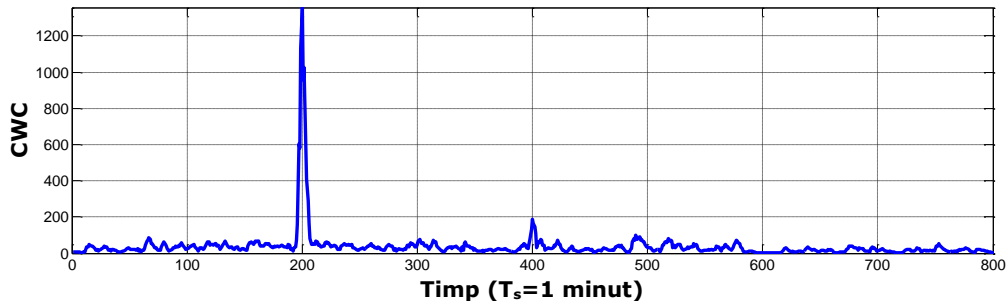


Figura 5.7. Semnalul CWC rezultat pentru semnalul de trafic din figura 5.5

Câteva observații interesante se desprind din figura 5.7. În primul rând, se vede că cumulantul Cum4 urmărește mult mai bine variațiile din semnalul de trafic. În momentele de timp unde sunt localizate cele două anomalii, valorile Cum4 obținute sunt 1357, respectiv 189,37. În plus, se poate observa că vârful din momentul de timp $t = 400$ (corespunzător anomaliei 2) este mult mai vizibil, în raport cu vârful corespunzător anomaliei din momentul de timp $t = 200$. O soluție clasică pentru a pune în evidență pe același desen cantități extreme de mărimi foarte diferite este modificarea axei verticale (wrapping). Raportul de proporționalitate între aceste două valori Cum4 este de doar 7,16, față de 64,91 în cazul varianței. Prin urmare, în această situație, mecanismul de alegere a pragurilor de detecție devine mai puțin critic. Tot în urma simulărilor efectuate, am constatat că mărimea Cum4 este mult mai puțin sensibilă în raport cu lungimea ferestrei de detecție considerată. Toate observațiile anterioare arată că folosirea mărimilor statistice de ordin ridicat poate conduce la obținerea unor rezultate mai bune în detecția anomaliilor din trafic.

În cele din urmă, procesul de detecție are ca scop localizarea în timp a anomaliilor detectate prin utilizarea unor praguri de decizie. Există câte un prag pentru fiecare nivel de descompunere. De asemenea, pragurile de filtrare se determină pentru fiecare tip de semnal caracteristic utilizat ca semnal de intrare. Niște praguri cu valori mari, determină o detecție cu un nivel ridicat de încredere a anomaliilor, precum și o reducere a alarmelor false.

5.9. Analiza performanțelor de detecție a anomaliilor

5.9.1. Parametrii de simulare și mărimile de evaluare a performanțelor

În evaluarea metodei de detecție propusă, am adoptat ca și trafic de date, setul de date "1999 DARPA/MIT Lincoln Intrusion Detection Dataset" [DARPA99], devenit un standard foarte des utilizat în evaluarea sistemelor de detecție a anomaliilor din traficul de rețea. Aceste date reprezintă traficul captat dintr-o rețea simulată, pe durata a cinci săptămâni, dintre care două săptămâni, conțin doar trafic normal fără nici un atac (pentru antrenarea sistemelor IDS). Traficul de date este disponibil sub forma unor fișiere în format *tcpdump*.

Analiza performanțelor de detecție este efectuată folosind traficul de date din prima zi a săptămânii patru (S4Z1). Pentru caracterizarea traficului din ziua

respectivă, vom utiliza mărimile caracteristice prezentate în tabelul 5.1. Aceste semnale cuprind fiecare un număr de 1024 eșantioane, intervalul de timp de eșantionare T_s fiind de 1 minut. În figura 5.8 sunt ilustrate câteva dintre aceste semnale utilizate în analiza traficului.

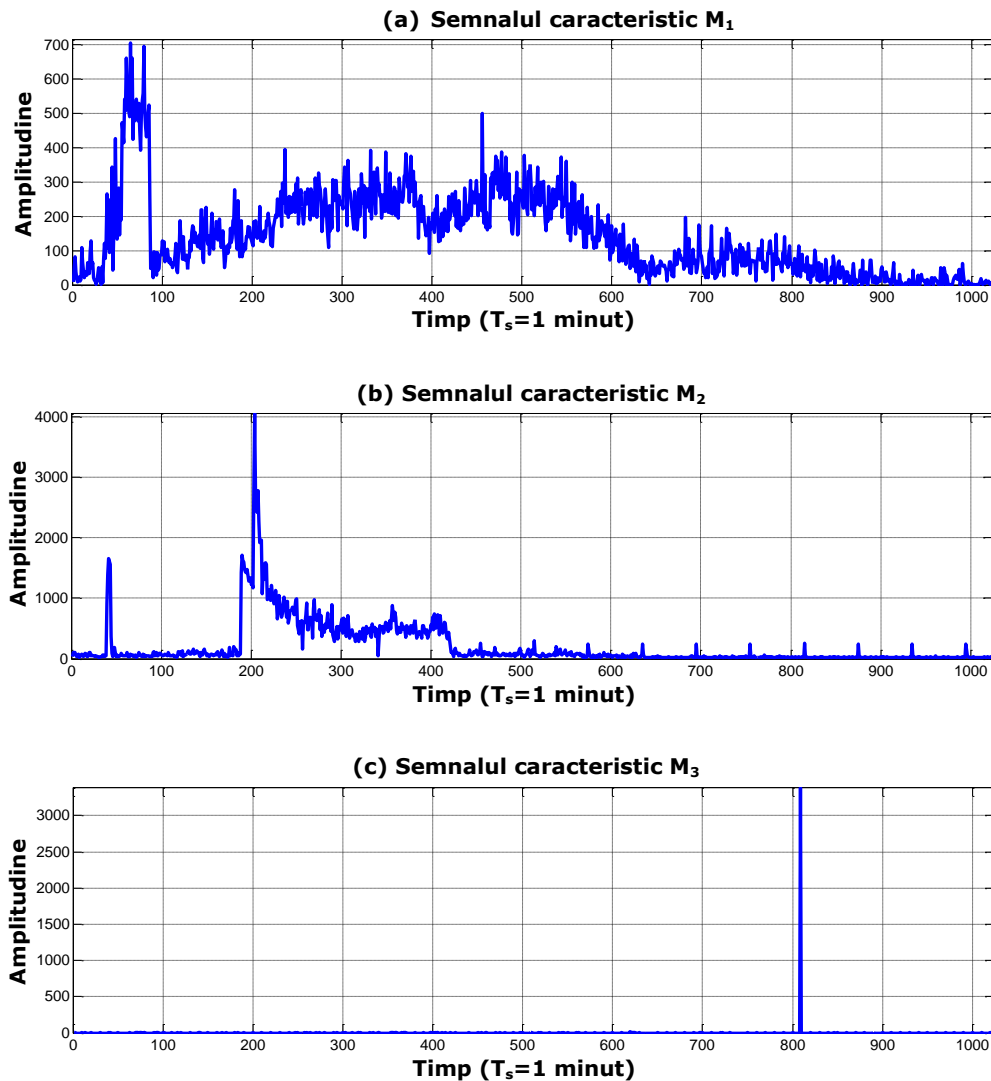


Figura 5.8. Numărul de fluxuri (a) TCP, (b) UDP și (c) ICMP într-un minut, pentru S4Z1

În traficul de date din S4Z1, sunt cuprinse un număr total de $N_a = 16$ anomalii, durata totală a acestora în eșantioane fiind $N_t = 130$ eșantioane. Momentul de început precum și durata efectivă a fiecărei anomalie sunt specificate în [DARPA99]. Parametrii anomaliilor care se regăsesc în S4Z1 sunt prezentați în tabelul 5.2.

Atac	Tipul Atacului	Durata Atacului (eșantioane)
1	Ps-u2r	47
2	Sendmail-r2l	1
3	Ntfstdos- r2l	9
4	PortswEEP- probe	1
5	SshTrojanInstall- r2l	1
6	PortswEEP- probe	5
7	Xsnoop-r2l	2
8	Snmpget-r2l	34
9	Guesstelnet-r2l	1
10	PortswEEP-probe	6
11	Guessftp-r2l	1
12	Ftpwrite-r2l	6
13	Crashiis-dos	2
14	PortswEEP- probe	5
15	Secret- data	9
16	Smurf- dos	1
TOTAL		130

Tabel 5.2. Parametrii tipurilor de anomalii din S4Z1, $T_s=1$ minut

Așa cum am văzut în paragraful anterior, detecția anomaliilor utilizând metoda propusă se bazează pe calculul transformării wavelet ASWT și a semnalului cumulant de ordinul patru. Există câțiva parametri importanți care trebuie luați în considerare: numărul de niveluri de descompunere (scări), lungimea ferestrei de detecție, tipul undișoarei mamă și pragurile de decizie. Valorile acestor parametri considerați în efectuarea simulărilor sunt redată în tabelul 5.3.

PARAMETRII DE SIMULARE	
Niveluri de descompunere	$J = 5$
Lungimea ferestrei de detecție L_{det}	$L_{det} = 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32$
Undișoara mamă ψ	Haar, Daubechies-4, 6, 8, Coiflet-1, 2, 3, Symmlet-4, 5, 6
Pragul de decizie λ	$\lambda = a \cdot m_{CWC}$, cu $a = 1, 1.5, 2, 2.5, 3$, unde m_{CWC} reprezintă media semnalului Cum4.
Mărimi caracteristice ale traficului de rețea	M_i , cu $i=1,2,3,4,5,6,7,8,9,10,11,12,13,14,15$

Tabel 5.3. Parametrii de simulare utilizați pentru evaluarea performanțelor de detecție

Rezultatele evaluărilor sunt prezentate și analizate având în vedere următoarele aspecte privind: numărul de eșantioane cu anomalii și numărul de

anomalii detectate în cazul fiecărei mărimi caracteristice a traficului, precum și în cazul corelării tuturor acestor mărimi, numărul de eșantioane identificate din fiecare anomalie. Astfel, vom considera mărimile de evaluare prezentate în relațiile următoare:

$$P_s = \text{Număr de eșantioane cu anomalii, corect detectate} \quad (5.5)$$

$$F_s = \text{Număr de eșantioane cu anomalii, fals detectate} \quad (5.6)$$

$$\frac{P_s}{F_s} \cdot 100 \quad (5.7)$$

$$DR_1 = \frac{\text{Număr de anomalii detectate}}{\text{Număr total de anomalii}} \cdot 100 \quad (5.8)$$

$$DR_2 = \frac{\text{Număr de eșantioane cu anomalii, corect detectate}}{\text{Număr total de eșantioane cu anomalii}} \cdot 100 \quad (5.9)$$

De asemenea, se vor analiza efectele asupra performanțelor obținute atunci când se dorește obținerea unui număr cât mai mic de alarme false, detecția unui număr maxim de eșantioane cu anomalii, a celui mai bun compromis între acestea două precum și obținerea unui număr nul de alarme false. Aceste criterii de căutare a parametrilor optimi pentru metoda propusă, presupun maximizarea mărimilor de evaluare. Aceste criterii de căutare sunt definite în relația 5.10:

$$\left\{ \begin{array}{l} \text{Criteriul 1(C1)} : \max \left\{ \frac{1}{F_s} \right\}, \\ \text{Criteriul 2(C2)} : \max \{ P_s \}, \\ \text{Criteriul 3(C3)} : \max \left\{ \frac{P_s}{F_s} \right\}, \\ \text{Criteriul 4(C4)} : F_s = 0. \end{array} \right. \quad (5.10)$$

Un sistem de detecție ideal, presupune detecția tuturor eșantioanelor cu anomalii din semnalul de trafic analizat și generarea unui număr nul de alarme false. În realitate, sistemele IDS generează cu o probabilitate mare, un număr de alarme false diferit de zero, un număr cu atât mai mare cu cât numărul de eșantioane cu anomalii identificate corect este mai mare.

Se studiază experimental, în cele ce urmează, care este influența acestor parametri asupra performanțelor de detecție a anomaliilor de trafic.

5.9.2. Rezultatele detecției la diferite scări

Pentru început, vom analiza rezultatele obținute în urma simulărilor efectuate pentru fiecare nivel de descompunere ASWT. Parametrii de simulare utilizați sunt cei ilustrați în tabelul 5.3, iar criteriile de căutare a parametrilor optimi sunt cele definite în relația 5.10. Scopul acestui studiu nu este însă atât de a face o analiză cantitativă, cât una calitativă.

La scara $J=1$, performanțele globale de detecție a anomaliilor sunt prezentate în tabelul 5.4. Acest tabel cuprinde rezultatele obținute individual utilizând cele 15 mărimi caracteristice introduse în tabelul 5.1, precum și rezultatele obținute prin corelarea tuturor acestor rezultate.

86 Aplicații ale RTF în detecția anomaliilor din traficul de rețea - 5

		P_s	F_s	P_s/F_s	DR ₁ /Anomalii detectate	DR ₂	L_{det}	α	ψ
M_1	C1	14	0	-	12.5/1,2	10.77	14	3	Daub-8
	C2	110	371	29.65	75/1,2,3,4,7,8,9,10,11,12,13,14	84.62	32	1	Daub-4
	C3	14	0	-	12.5/1,2	10.77	14	3	Daub-8
M_2	C1	24	26	92.31	25/1,6,7,8	18.46	12	3	Haar
	C2	92	323	28.48	75/1,2,6,7,8,9,10,11,12,14,15,16	70.77	18	1	Coif-2
	C3	36	30	120	37.5/1,2,6,7,8,10	27.69	20	2.5	Coif-2
M_3	C1	1	2	50.00	6.25/16	0.77	2	2	Haar
	C2	10	14	71.43	18.75/1,3,12	7.69	6	1	Haar
	C3	10	14	71.43	18.75/1,3,12	7.69	6	1	Haar
M_4	C1	7	16	43.75	6.25/1	5.38	8	3	Coif-1
	C2	40	322	12.42	56.25/1,2,7,8,10,12,13,14,15	30.77	4	1	Coif-2
	C3	10	20	50.00	6.25/1	7.69	12	3	Coif-3
M_5	C1	2	0	-	12.5/8,10	1.53	20	3	Coif-3
	C2	102	302	33.77	62.5/1,2,3,4,8,9,11,14,15,16	78.46	32	1	Daub-4
	C3	21	2	1050	12.5/8,10	16.15	30	2.5	Coif-3
M_6	C1	8	18	44.44	18.75/1,8,16	6.15	2	3	Haar
	C2	67	194	34.54	50/1,2,3,4,5,8,9,16	51.54	32	1	Daub-8
	C3	42	81	51.85	25/1,2,8,16	32.31	20	2	Daub-4
M_7	C1	9	55	16.36	12.5/1,14	6.92	2	3	Haar
	C2	56	196	28.57	56.25/1,2,3,4,5,8,12,14,15	43.08	6	1	Haar
	C3	56	196	28.57	56.25/1,2,3,4,5,8,12,14,15	43.08	6	1	Haar
M_8	C1	12	0	-	6.25/8	9.23	26	3	Daub-8
	C2	83	316	26.27	43.75/1,3,8,11,14,15,16	63.85	30	1	Daub-8
	C3	12	0	-	6.25/8	9.23	26	3	Daub-8
M_9	C1	12	12	100	12.5/8,16	9.23	12	3	Haar
	C2	56	319	17.55	62.5/1,3,5,6,8,10,12,14,15,16	43.08	2	1	Haar
	C3	12	12	100	12.5/8,16	9.23	12	3	Haar
M_{10}	C1	5	28	17.86	12.5/1,5	3.85	14	3	Sym-6
	C2	87	364	23.90	75/1,2,3,4,5,6,7,11,12,13,14,15	66.92	32	1	Haar
	C3	26	58	44.83	31.25/1,2,5,8,15	20	6	2.5	Sym-4
M_{11}	C1	20	0	-	6.25/1	15.38	22	2.5	Haar
	C2	98	428	22.90	75/1,2,3,4,5,8,9,11,13,14,15,16	75.38	32	1	Daub-8
	C3	20	0	-	6.25/1	15.38	22	2.5	Haar
M_{12}	C1	4	7	57.14	18.75/3,4,16	3.08	8	3	Daub-6
	C2	93	270	34.44	56.25/1,2,3,8,10,11,12,15,16	71.54	30	1	Daub-4
	C3	15	20	75.00	37.5/1,3,4,8,12,16	11.54	6	2.5	Daub-4
M_{13}	C1	0	0	-	6.25/14	0.77	12	3	Coif-1
	C2	70	385	18.18	68.75/6,7,8,9,10,11,12,13,14,15,16	53.58	14	1	Daub-6
	C3	1	0	-	6.25/14	0.77	12	3	Coif-1
M_{14}	C1	22	22	100	25/1,6,7,10	16.92	10	3	Haar
	C2	94	346	27.17	75/1,2,6,7,8,9,10,11,12,14,15,16	72.31	24	1	Coif-2

5.9 – Analiza performanțelor de detecție a anomaliilor 87

	C3	41	35	117.1	37.5/1,2,6,7,8,10	31.54	22	2.5	Sym-5
M ₁₅	C1	1	4	25.00	6.25/16	0.77	2	3	Haar
	C2	30	132	22.73	43.75/1,3,4,8,12,13,15	23.08	6	1	Haar
	C3	7	21	33.33	31.25/1,8,12,14,16	5.38	2	1.5	Haar
Cor M _i	C1	71	139	51.08	68.75/1,2,3,4,5,6,7,8, 10,14,16	54.61			
	C2	128	876	14.61	100/1,2,3,4,5,6,7,8,9, 10,11,12,13,14,15,16	98.46	-	-	-
	C3	112	324	34.57	81.28/1,2,3,4,5,6,7,8, 10,12,14,15,16	86.15			
	C4	44	0	-	31.25/1,2,8,10,14	33.84			

Tabel 5.4. Performanțele de detecție ale anomaliilor pentru S4Z1, la scara J=1

Analiza rezultatelor din tabelul 5.4 dezvăluie câteva concluzii interesante. Astfel, prin corelarea rezultatelor obținute în cazul celor 15 mărimi caracteristice se obțin rezultatele cele mai bune, indiferent de criteriul de evaluare avut în vedere. Într-adevăr, putem observa că metoda propusă identifică toate tipurile de anomalii conținute în semnalul de trafic analizat, iar din numărul total de 130 de eşantioane cu anomalii, se detectează un număr de 128 de eşantioane. De asemenea, metoda de detecție identifică corect 44 de eşantioane cu anomalii, fără generarea de alarme false. Performanța globală $\frac{P_S}{F_S}$ cea mai bună se obține atunci când pentru mărimile

M_i se ia în considerare criteriul C1. O altă observație interesantă este legată de legătura care există între pragurile de decizie și lungimea ferestrei de detecție. Utilizarea unui prag mic ($a=1$) are ca efect pe de o parte, detecția unui număr P_S mai mare, și pe de altă parte generarea unui număr mai mare de alarme false. Prin utilizarea unui prag mai mare ($a=3$) se constată minimizarea numărului de alarme false, în timp ce un prag intermediar ($a=2$) determină obținerea celui mai bun compromis între numărul maxim de alarme pozitive și numărul minim de alarme negative detectate. Maximizarea mărimii $\frac{1}{F_S}$ se obține prin utilizarea unei ferestre de detecție L_{det} mare, maximizarea mărimii $\frac{1}{F_S}$ pentru o lungime L_{det} mică, iar maximizarea mărimii $\frac{P_S}{F_S}$ pentru o lungime medie a feretrei de detecție.

Având în vedere rezultatele de mai sus, putem afirma următoarele: pentru detecția corectă a unui număr cât mai mare de eşantioane cu anomalii (dar cu un număr mai mare de alarme false) se poate folosi o fereastră de detecție de lungime mare și un prag de decizie mic; pentru detecția unui număr cât mai mic de alarme false se poate utiliza o fereastră de detecție de lungime mică și a unui prag de decizie mare; pentru obținerea celui mai bun compromis între cazurile anterioare, se poate folosi o fereastră de detecție și un prag de decizie de valori medii. În ceea ce privește tipul undișoarelor mamă selectate, se observă că pentru criteriile de evaluare C1, C2 și C3, undișoara mamă aleasă cel mai des este undișoara mamă Haar.

Pentru ilustrare, în figura 5.9 este prezentat unul din rezultatele detecției. Linia punctată orizontală constituie pragul de decizie, în timp ce localizarea temporală a anomaliilor detectate este ilustrată prin liniile punctate vertical. Anomaliile identificate sunt: 1, 5, 8, 11.

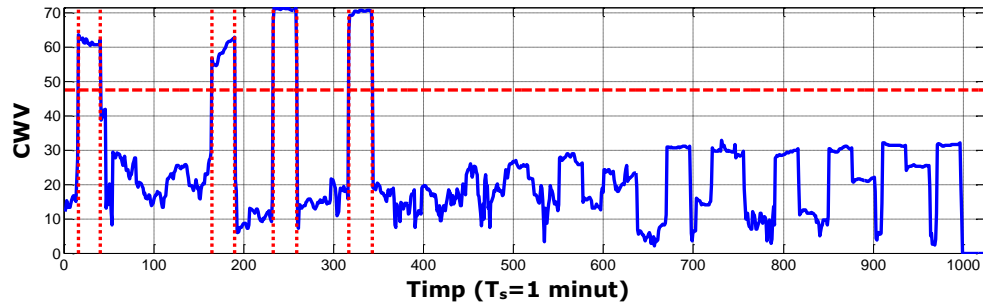


Figura 5.9. Rezultatul detecției pentru S4Z1, la scara $J=1$, pentru M_8 , cu Daubechies-8, $L_{det}=26$, $\alpha=2$

În tabelul 5.5 sunt redate rezultatele detecției la scara $J=2$.

		P_s	F_s	P_s/F_s	DR ₁ /Anomalii detectate	DR ₂	L_{det}	α	ψ
M_1	C1	2	0	-	12.5/3,4	1.54	20	3	Daub-6
	C2	101	294	34.35	68.75/1,2,3,4,8,9,10, 11,12,13,14	77.69	30	1	Daub-4
	C3	2	0	-	12.5/3,4	1.54	20	3	Daub-6
M_2	C1	33	27	122.2	37.5/1,6,7,8,9,10	25.38	8	3	Haar
	C2	89	124	71.77	50/1,2,6,7,8,9,10,12	68.46	22	1	Coif-3
	C3	72	47	153.1 9	43.75/1,2,6,7,8,9,10	55.38	20	2	Coif-3
M_3	C1	1	4	25.00	6.25/16	0.77	2	1.5	Haar
	C2	1	5	20.00	6.25/16	0.77	2	1	Haar
	C3	1	4	25.00	6.25/16	0.77	2	1.5	Haar
M_4	C1	10	23	43.48	6.25/1	7.69	6	3	Coif-2
	C2	42	188	22.34	37.5/1,3,4,6,7,16	32.31	30	1	Daub-8
	C3	14	26	53.85	6.25/1	10.77	4	3	Coif-3
M_5	C1	0	1	0.00	0	0	28	3	Daub-6
	C2	96	380	25.26	68.75/1,2,3,4,6,8,11, 13,14,15,16	73.85	24	1	Sym-4
	C3	13	3	433.3	18.75/1,2,6	10	14	3	Coif-3
M_6	C1	9	30	30.00	18.75/1,8,16	6.92	2	3	Haar
	C2	69	337	20.47	75/1,2,3,4,5,6,8,10,12, 14,15,16	53.08	6	1	Haar
	C3	63	132	47.73	50/1,3,5,8,10,12,14,16	48.46	14	1	Haar
M_7	C1	13	51	25.49	6.25/1	10	6	3	Coif-3
	C2	64	277	23.10	68.75/1,2,3,4,5,6,7,8, 11,12,14	49.23	12	1	Daub-8
	C3	54	200	27.00	56.25/2,3,4,5,8,11,12, 14	41.54	6	1	Haar
M_8	C1	6	0	-	6.25/1	4.62	32	3	Daub-6
	C2	99	341	29.03	62.5/1,2,3,4,6,8,9,11, 15,16	76.15	32	1	Daub-8
	C3	6	0	-	6.25/1	4.62	32	3	Daub-6
M_9	C1	1	12	8.33	6.25/16	0.77	10	3	Haar
	C2	60	178	33.71	56.25/1,3,4,5,8,10,12, 15,16	46.15	12	1	Haar
	C3	30	56	53.57	43.75/1,3,4,8,12,15,16	23.08	4	1.5	Haar

5.9 – Analiza performanțelor de detecție a anomaliilor 89

M ₁₀	C1	0	2	0.00	0	0	26	3	Sym-5
	C2	90	332	27.11	75/1,2,3,4,5,6,7,8,11, 12,14,15	69.23	14	1	Daub-8
	C3	64	154	41.56	43.75/1,2,5,6,7,14,15	48.46	18	1.5	Sym-5
M ₁₁	C1	30	0	-	6.25/1	23.08	30	2	Daub-8
	C2	104	403	25.81	68.75/1,2,3,4,6,8,10, 11,14,15,16	80	32	1	Coif-3
	C3	30	0	-	6.25/1	23.08	30	2	Daub-8
M ₁₂	C1	6	7	85.71	12.5/3,16	4.62	16	3	Daub-8
	C2	79	274	28.83	68.75/1,2,3,4,5,8,10, 11,12,15,16	60.77	32	1	Daub-6
	C3	19	14	135.7	31.25/3,4,12,15,16	14.62	6	3	Daub-6
M ₁₃	C1	0	1	0.00	0	0	16	3	Haar
	C2	61	441	13.83	56.25/6,7,8,9,10,11, 12,13,14	46.92	30	1	Daub-4
	C3	1	1	100.0	6.25/11	0.77	12	3	Sym-4
M ₁₄	C1	28	26	107.6	31.25/1,6,7,8,10	21.54	8	3	Haar
	C2	90	202	44.55	68.75/1,2,6,7,8,9,10, 11,12,14,15	69.23	16	1	Sym-6
	C3	52	34	152.9	43.75/1,2,6,7,8,9,10	40	14	2.5	Coif-1
M ₁₅	C1	1	4	25.00	6.25/16	0.77	2	3	Haar
	C2	11	40	27.50	43.75/1,3,5,8,12,14,16	8.46	2	1	Haar
	C3	11	40	27.50	43.75/1,3,5,8,12,14,16	8.46	2	1	Haar
Cor M _i	C1	65	127	51.18	56.25/1,3,4,6,7,8,9,10, 16	50			
	C2	128	859	14.90	100/1,2,3,4,5,6,7,8,9, 10,11,12,13,14,15,16	98.46	-	-	-
	C3	126	405	31.11	93.75/1,2,3,4,5,6,7,8, 9,10,11,12,14,15,16	96.92			
	C4	32	0	-	18.75/1,3,4	24.61			

Tabel 5.5. Performanțele de detecție ale anomaliilor pentru S4Z1, la scara J=2

Analizând rezultatele din tabelul 5.5, putem constata în primul rând, performanțe globale asemănătoare cu cele obținute la scara $J=1$. De asemenea, pentru M_1 se obține, încă o dată, cea mai mare rată de detecție a eşantioanelor cu anomalii. Dintre familiile de undișoare utilizate, familia de undișoare Daubechies este selectată cel mai des, în particular undișoara Haar.

Figura 5.10 ilustrează rezultatul detecției pentru M_1 . Anomaliile identificate sunt: 1, 2, 3, 4, 8, 9, 10, 11, 12, 13, 14.

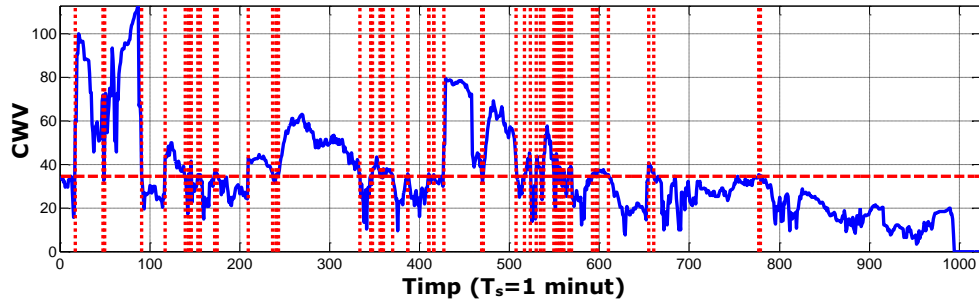


Figura 5.10. Rezultatul detecției pentru S4Z1, la scara $J=2$, pentru M_1 , cu Daubechies-4, $L_{det}=30$, $\alpha=1$

La scara $J=3$, rezultatele obținute sunt prezentate în tabelul 5.6.

		P_s	F_s	P_s/F_s	DR ₁ /Anomalii detectate	DR ₂	L_{det}	α	ψ
M_1	C1	1	5	20.00	6.25/5	0.77	30	3	Coif-3
	C2	112	352	31.82	75/1,2,3,4,5,6,7,8,9,10,12,14	86.15	32	1	Sym-4
	C3	46	18	255.5	25/1,2,3,4	35.38	32	2	Haar
M_2	C1	31	27	114.8	37.5/1,2,6,7,8,12	23.85	4	3	Daub-4
	C2	95	136	69.85	56.25/1,2,6,7,8,9,10,11,12	73.08	24	1	Daub-8
	C3	63	41	153.6	31.25/1,2,6,7,8	48.46	24	2	Coif-1
M_3	C1	1	8	12.50	6.25/16	0.77	2	1.5	Haar
	C2	1	9	11.11	6.25/16	0.77	2	1	Haar
	C3	1	8	12.50	6.25/16	0.77	2	1.5	Haar
M_4	C1	9	24	37.50	6.25/1	6.92	6	3	Sym-5
	C2	35	280	12.50	43.75/1,3,4,6,7,12,15	26.92	18	1	Sym-4
	C3	10	26	38.46	6.25/1	7.69	6	3	Haar
M_5	C1	36	7	514.2	18.75/1,2,6	27.69	26	3	Coif-3
	C2	99	205	48.29	62.5/1,2,3,4,6,7,8,11,13,14	76.15	32	1	Daub-6
	C3	36	7	514.2	18.75/1,2,6	27.69	26	3	Coif-3
M_6	C1	0	20	0.00	0	0	24	3	Haar
	C2	74	212	34.91	68.75/1,2,3,4,5,8,9,12,13,14,15,16	56.92	24	1	Haar
	C3	45	110	40.91	25/1,8,9,16	34.62	26	1.5	Haar
M_7	C1	8	36	22.22	6.25/1	6.15	24	3	Haar
	C2	69	288	23.96	62.5/1,2,3,4,5,6,7,11,12,14	53.08	16	1	Daub-6
	C3	66	273	24.18	62.5/1,2,3,4,5,6,7,11,12,14	50.77	12	1	Daub-6
M_8	C1	42	12	350.0	18.75/1,2,6	32.31	26	3	Coif-2
	C2	92	144	63.89	50/1,2,3,4,6,8,10,11	70.77	32	1	Daub-4
	C3	42	12	350	18.75/1,2,6	32.31	26	3	Coif-2
M_9	C1	1	17	5.88	6.25/16	0.77	12	3	Haar
	C2	60	190	31.58	62.5/1,3,4,5,8,9,11,12,15,16	46.15	24	1	Haar
	C3	25	48	52.08	31.25/3,8,12,15,16	19.23	6	2	Coif-2
	C1	2	0	-	6.25/1	1.54	32	3	Daub-6

5.9 – Analiza performanțelor de detecție a anomaliilor 91

M ₁₀	C2	85	378	22.49	75/1,2,3,4,5,6,7,11,12,13,14,15	65.38	30	1	Haar
	C3	35	5	700.0	25/1,2,3,4	27.69	32	2.5	Haar
M ₁₁	C1	35	0	-	18.75/1,2,6	26.92	28	3	Sym-5
	C2	98	239	41.00	62.5/1,2,3,4,5,6,8,11,14,15	75.38	28	1	Daub-4
	C3	35	0	-	18.75/1,2,6	26.92	28	3	Sym-5
M ₁₂	C1	5	3	166.6	6.25/15	3.85	32	3	Daub-4
	C2	73	216	33.80	62.5/1,2,3,5,11,12,13,14,15,16	56.15	32	1	Coif-1
	C3	5	3	166.6	6.25/15	3.85	32	3	Daub-4
M ₁₃	C1	0	1	0.00	0	0	32	3	Sym-5
	C2	61	423	14.42	56.25/6,7,8,9,10,11,12,13,14	46.92	30	1	Coif-3
	C3	1	2	50.00	6.25/11	0.77	16	3	Haar
M ₁₄	C1	29	27	107.4	31.25/1,2,6,7,8	22.31	8	3	Sym-6
	C2	95	143	66.43	56.25/1,2,6,7,8,9,10,11,12	73.08	26	1	Daub-8
	C3	61	38	160.5	31.25/1,2,6,7,8	46.92	24	2	Coif-1
M ₁₅	C1	1	8	12.50	6.25/16	0.77	2	2.5	Haar
	C2	8	19	42.11	25/1,3,15,16	6.15	2	1	Haar
	C3	8	19	42.11	25/1,3,15,16	6.15	2	1	Haar
Cor M _i	C1	61	141	43.26	56.25/1,2,5,6,7,8,12,15,16	46.92	-	-	-
	C2	128	793	16.14	100/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	98.46	-	-	-
	C3	119	404	29.46	87.5/1,2,3,4,5,6,7,8,9,11,12,14,15,15	91.53	-	-	-
	C4	35	0	-	18.75/1,2,6	26.92	-	-	-

Tabel 5.6. Performanțele de detecție ale anomaliilor pentru S4Z1, la scara $J=3$

Comparativ, performanțele globale de detecție redată în tabelul 5.6 sunt puțin inferioare performanțelor rezultate la scările 1 și 2. Totuși, se constată o scădere a alarmelor false F_S (la 793 de eşantioane) în cazul detecției numărului maxim P_S (128 de eşantioane).

Figura 5.11 ilustrează rezultatul detecției pentru M_{11} . Anomaliile identificate sunt: 1, 2, 6.

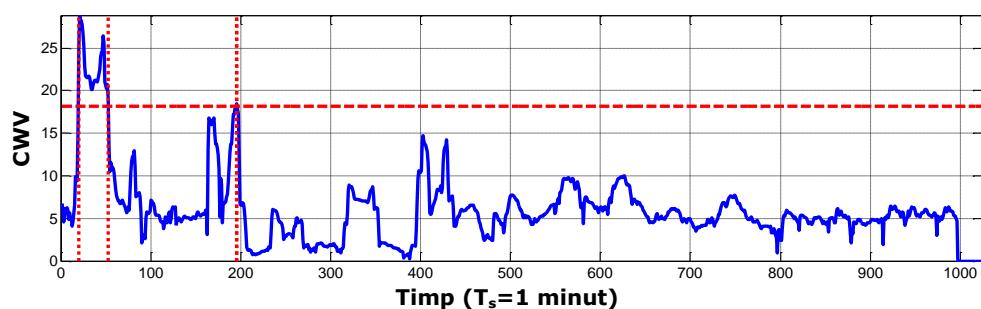


Figura 5.11. Rezultatul detecției pentru S4Z1, la scara $J=3$, pentru M_{11} , cu Symmlet-5, $L_{det}=28$, $\alpha=3$

La scara $J=4$, rezultatele obținute sunt prezentate în tabelul 5.7.

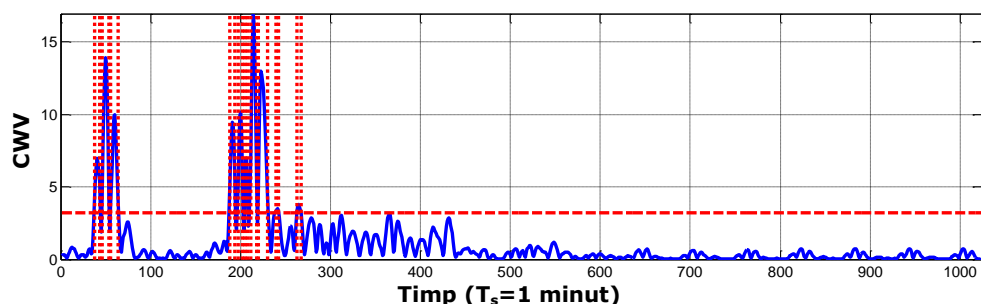
		P_s	F_s	P_s/F_s	DR_1 /Anomalii detectate	DR_2	L_{de} t	α	ψ
M_1	C1	20	16	125.00	12.5/1,5	15.38	8	3	Haar
	C2	87	287	30.31	62.5/1,2,3,4,5,6,8,9, 13,14	66.92	12	1	Sym-4
	C3	47	22	213.64	31.25/1,2,3,4,5	36.15	32	2.5	Daub-8
M_2	C1	40	27	148.15	50/1,2,3,6,7,8,9,10	30.77	2	3	Coif-3
	C2	106	185	57.30	62.5/1,2,3,6,7,8,9,10, 11,12	81.54	18	1	Daub-8
	C3	48	30	160.00	43.75/1,2,6,7,8,9,10	36.92	6	3	Sym-4
M_3	C1	1	16	6.25	6.25/16	0.77	2	1	Haar
	C2	1	16	6.25	6.25/16	0.77	2	1	Haar
	C3	1	16	6.25	6.25/16	0.77	2	1	Haar
M_4	C1	0	30	0.00	0	0	30	3	Daub-8
	C2	52	269	19.33	43.75/1,2,8,9,10,15,16	40	2	1	Daub-8
	C3	20	37	54.05	6.25/1	15.38	12	3	Daub-6
M_5	C1	39	14	278.57	18.75/1,2,6	30	32	3	Coif-1
	C2	100	230	43.48	62.5/1,2,3,4,6,7,8,11, 12,15	76.92	28	1	Daub-8
	C3	39	14	278.57	18.75/1,2,6	30	32	3	Coif-1
M_6	C1	1	53	1.89	6.25/16	0.77	28	3	Daub-4
	C2	73	292	25.00	75/1,2,3,4,5,8,9,10,11, 12,15,16	56.15	28	1	Coif-1
	C3	72	235	30.64	56.25/1,3,4,5,8,10,12, 15,16	55.38	20	1	Haar
M_7	C1	6	29	20.69	6.25/1	4.62	32	3	Coif-1
	C2	71	287	24.74	56.25/1,2,3,4,5,6,7,11, 12	54.62	24	1	Haar
	C3	24	43	55.81	12.5/1,5	18.46	14	3	Coif-3
M_8	C1	23	20	115.00	18.75/1,2,6	17.69	2	3	Haar
	C2	108	172	62.79	62.5/1,2,3,4,6,7,8,11, 12,15	83.08	30	1	Daub-8
	C3	37	20	185.00	18.75/1,2,6	28.46	28	3	Daub-8
M_9	C1	6	27	22.22	18.75/12,15,16	4.62	12	3	Haar
	C2	60	186	32.26	56.25/1,2,3,4,8,11,12, 15,16	46.15	32	1	Haar
	C3	29	72	40.28	37.5/3,4,8,12,15,16	22.31	12	2	Haar
M_{10}	C1	17	15	113.33	6.25/1	13.08	32	3	Daub-6
	C2	101	291	34.71	75/1,2,3,4,5,6,7,8,11, 12,14,15	77.69	30	1	Daub-6
	C3	17	15	113.33	6.25/1	13.08	32	3	Daub-6
M_{11}	C1	33	6	550.00	12.5/1,2	25.38	32	3	Sym-5
	C2	83	162	51.23	62.5/1,2,3,4,6,7,8,14, 15,16	63.85	18	1	Sym-4
	C3	33	6	550.00	12.5/1,2	25.38	32	3	Sym-5
M_{12}	C1	24	42	57.14	37.5/3,4,5,12,15,16	18.46	4	3	Daub-4
	C2	62	247	25.10	56.25/1,2,3,4,5,11,12, 15,16	47.69	32	1	Coif-1
	C3	36	56	64.29	43.75/1,2,3,4,11,12,15	27.69	32	3	Haar
M_{13}	C1	5	0	-	6.25/12	3.85	28	3	Daub-6
	C2	61	391	15.60	56.25/6,7,8,9,10,11, 12,13,14	46.92	20	1	Haar
	C3	5	0	-	6.25/12	3.85	28	3	Daub-6

M_{14}	C1	43	26	165.38	43.75/1,2,6,7,8,9,10	33.08	2	3	Sym-5
	C2	106	178	59.55	62.5/1,2,3,6,7,8,9,10,11,12	81.54	18	1	Daub-8
	C3	43	26	165.38	43.75/1,2,6,7,8,9,10	33.08	2	3	Sym-5
M_{15}	C1	1	16	6.25	6.25/16	0.77	2	2	Haar
	C2	9	21	42.86	18.75/12,15,16	6.92	2	1	Haar
	C3	9	21	42.86	18.75/12,15,16	6.92	2	1	Haar
$Cor M_i$	C1	98	222	44.14	81.25/1,2,3,4,5,6,7,8,9,10,12,15,16	75.38	-	-	-
	C2	128	794	16.12	100/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	98.46	-	-	-
	C3	121	360	33.61	87.5/1,2,3,4,5,6,7,8,9,10,11,12,15,16	93.07	-	-	-
	C4	5	0	-	6.25/12	3.84	-	-	-

Tabel 5.7. Performanțele de detecție ale anomaliilor pentru S4Z1, la scara $J=4$

Analizând rezultatele obținute pentru scara 4, putem nota faptul că și pe acest nivel de descompunere, rata de detecție DR_2 este de 98,46 % identificându-se toate tipurile de anomalii. În plus, putem observa încă o dată că, indiferent de criteriul de căutare considerat, pentru undișoara mamă Haar se obțin de cele mai multe ori performanțele optime.

Figura 5.12 ilustrează rezultatul detecției pentru M_{14} . Anomaliile identificate sunt: 1, 2, 6, 7, 8, 9, 10.

Figura 5.12. Rezultatul detecției pentru S4Z1, la scara $J=4$, pentru M_{14} , cu Symmlet-5, $L_{det}=2$, $\alpha=3$

La scara $J=5$, rezultatele obținute sunt prezentate în tabelul 5.8.

		P_s	F_s	P_s/F_s	DR_1 /Anomalii detectate	DR_2	L_{det}	α	ψ
M_1	C1	32	27	118.5	31.25/1,2,3,4,5	24.62	10	3	Haar
	C2	89	199	44.72	62.5/1,2,3,4,5,8,9,12,13,14	68.46	28	1	Sym-5
	C3	47	27	174.0	31.25/1,2,3,4,5	36.15	32	3	Coif-1
M_2	C1	40	30	133.3	43.75/1,2,3,6,7,8,9	30.77	6	3	Daub-8
	C2	109	145	75.17	62.5/1,2,3,4,6,7,8,9,10,12	83.85	24	1	Daub-4
	C3	52	32	162.5	31.25/1,6,7,8,9	40	2	3	Daub-6
M_3	C1	1	32	3.13	6.25/16	0.77	2	1	Haar
	C2	1	32	3.13	6.25/16	0.77	2	1	Haar

94 Aplicații ale RTF în detecția anomaliilor din traficul de rețea - 5

	C3	1	32	3.13	6.25/16	0.77	2	1	Haar
M ₄	C1	30	23	130.4	12.5/1,2	23.08	2	3	Daub-6
	C2	71	259	27.41	37.5/1,2,5,8,9,15	54.62	6	1	Coif-3
	C3	33	24	137.5	12.5/1,2	25.38	12	3	Sym-5
M ₅	C1	31	47	65.96	31.25/1,2,3,6,7	23.85	2	3	Haar
	C2	93	210	44.29	56.25/1,2,3,4,5,6,7,8,9	71.54	10	1	Coif-3
	C3	47	55	85.45	37.5/1,2,6,7,8,9	36.15	20	3	Daub-8
M ₆	C1	1	41	2.44	6.25/16	0.77	30	3	Daub-6
	C2	77	333	23.12	56.25/1,3,4,8,9,10,12,15,16	59.23	32	1	Daub-8
	C3	28	104	26.92	25/8,10,16,16	21.54	22	2	Daub-4
M ₇	C1	37	23	160.8	12.5/1,2	28.46	32	3	Coif-1
	C2	82	235	34.89	43.75/1,2,3,4,5,8,9	63.08	10	1	Coif-1
	C3	37	23	160.8	12.5/1,2	28.46	32	3	Coif-1
M ₈	C1	31	47	65.96	31.25/1,2,3,6,7	23.85	4	3	Haar
	C2	93	180	51.67	56.25/1,2,3,4,5,6,7,8,9	71.54	10	1	Coif-3
	C3	38	48	79.17	25/1,2,6,7	29.23	20	3	Haar
M ₉	C1	1	34	2.94	6.25/16	0.77	6	3	Haar
	C2	51	194	26.29	43.75/1,3,4,8,12,15,16	39.23	24	1	Haar
	C3	23	67	34.33	31.25/3,4,12,15,16	17.69	18	2	Haar
M ₁₀	C1	51	23	221.7	31.25/1,2,3,4,5	39.23	32	3	Coif-1
	C2	103	194	53.09	56.25/1,2,3,4,5,8,9,10,15	79.23	32	1	Sym-4
	C3	57	25	228.0	31.25/1,2,3,4,5	43.85	30	2	Coif-1
M ₁₁	C1	20	41	48.78	18.75/1,6,7	15.38	16	3	Coif -1
	C2	90	233	38.63	68.75/1,2,3,4,5,6,7,8,9,13,15	69.23	8	1	Sym-5
	C3	38	49	77.55	25/1,2,6,7	29.23	22	2.5	Haar
M ₁₂	C1	22	56	39.29	31.25/1,3,4,12,15	16.92	12	3	Daub-8
	C2	61	264	23.11	56.25/1,2,3,4,5,11,12,15,16	46.92	24	1	Daub-8
	C3	33	59	55.93	31.25/1,3,4,12,15	25.38	32	3	Coif
M ₁₃	C1	0	15	0.00	0	0	26	3	Haar
	C2	97	394	24.62	68.75/1,2,3,4,5,8,9,10,12,13,15	74.62	32	1	Haar
	C3	89	296	30.07	56.25/1,2,3,4,8,10,12,13,14	68.46	32	1	Coif-1
M ₁₄	C1	40	29	137.9	25/1,3,6,8	30.77	2	3	Daub-8
	C2	108	170	63.53	62.5/1,2,3,4,6,7,8,9,10,12	83.08	20	1	Daub-8
	C3	51	30	170.0	31.25/1,6,7,8,9	39.23	2	3	Daub-6
M ₁₅	C1	1	32	3.13	6.25/16	0.77	2	1.5	Haar
	C2	2	38	5.26	12.5/15,16	1.54	2	1	Haar
	C3	2	38	5.26	12.5/15,16	1.54	2	1	Haar
Cor M _i	C1	103	255	40.39	75/1,2,3,4,5,6,7,8,9,12,15,16	79.23	-	-	-
	C2	127	739	17.19	100/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	97.69	-	-	-
	C3	127	485	26.19	93.75/1,2,3,4,5,6,7,8,9,10,12,13,14,15,16	97.69	-	-	-
	C4	0	0	-	0	0	-	-	-

Tabel 5.8. Performanțele de detecție ale anomaliilor pentru S4Z1, la scara J=5

Analizând rezultatele din tabelul 5.8 putem spune că, rata de detecție DR_2 scade, în comparație cu celelalte scări. Totuși, sunt identificate în proporție de 100 %, toate tipurile de anomalii. În figura 5.13 este prezentat rezultatul detecției utilizând semnalul caracteristic M_2 . Anomaliile identificate sunt: 1, 2, 3, 4, 6, 7, 8, 9, 10, 12.

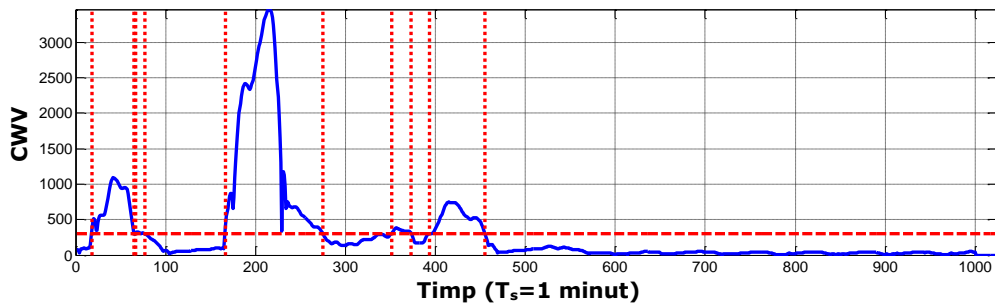


Figura 5.13. Rezultatul detecției pentru S4Z1, la scara $J=5$, pentru M_2 , cu Daubechies-4, $L_{det}=24$, $a=1$

Având la dispoziție rezultatele obținute pentru fiecare din cele 5 scări, se va face în continuare, o analiză comparativă a performanțelor globale obținute prin corelare. Cu alte cuvinte, vrem să vedem, în funcție de criteriul de selecție al parametrilor considerat, ce nivel de descompunere furnizează cele mai bune performanțe. În acest scop, vom considera patru criterii importante de evaluare. Primul, îl constituie numărul minim de eșantioane cu anomalii, fals detectate, F_S . Al doilea criteriu, este numărul maxim de eșantioane cu anomalii corect detectate, P_S . Criteriul trei, urmărește obținerea celui mai mare număr P_S posibil și a celui mai mic număr F_S posibil, fiecare dintre acestea având o pondere egală. Cu alte cuvinte, cel de-al treilea criteriu presupune găsirea celui mai mare raport $\frac{P_S}{F_S}$. Ultimul criteriu considerat, presupune pe de o parte, determinarea celei mai mari rate de detecție DR_2 și pe de altă parte, a celei mai mari valori a raportului $\frac{P_S}{F_S}$, fiecare cu o pondere egală. De fapt, criteriul patru urmărește maximizarea mărimii: $\frac{1}{2} \cdot DR_2 + \frac{1}{2} \cdot \frac{P_S}{F_S}$.

În figura 5.14 (a) sunt reprezentate rezultatele obținute privind numărul minim de alarme false detectate F_S , pe cele 5 scări. Performanța cea mai bună este indicată printr-un cerc colorat. De asemenea, în figura 5.14 (b) este ilustrată și performanța $\frac{P_S}{F_S}$ corespunzătoare.

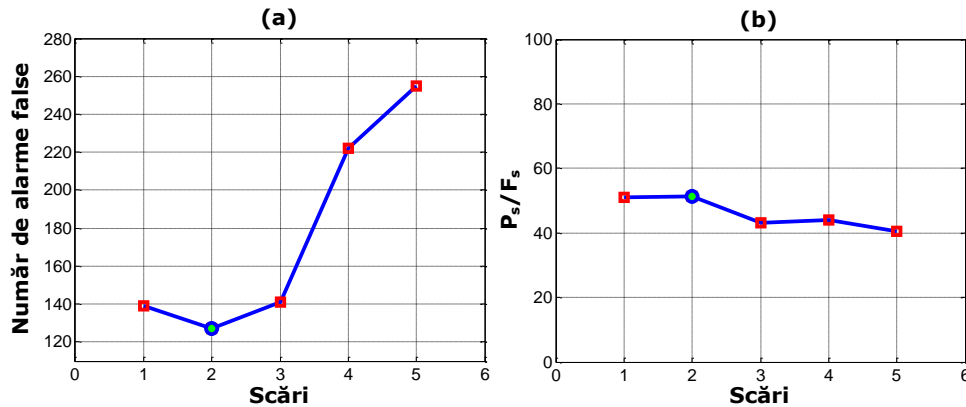


Figura 5.14. Performanța F_s (a) și P_s/F_s corespunzătoare (b), pe cele 5 scări

Analizând figura 5.14, putem constata că cele mai bune performanțe sunt obținute la scara $J=2$: $F_s=127$ și $\frac{P_s}{F_s}=51,18\%$.

Rezultatele obținute în cazul detecției numărului maxim de eșantioane cu anomalii P_s , sunt ilustrate în figura 5.15. Performanțele cele mai bune sunt indicate prin cercuri colorate.

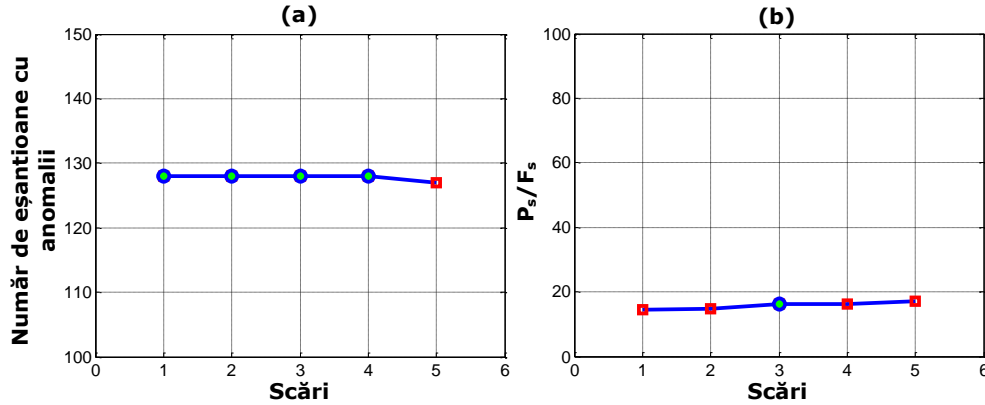


Figura 5.15. Performanța P_s (a) și P_s/F_s corespunzătoare (b), pe cele 5 scări

Din figura 5.15 (a) se observă că, la scările 1, 2, 3 și 4 se obține un număr de 128 de eșantioane cu anomalii corect detectate (dintr-un total de 130 de eșantioane). Dintre aceste scări, privind figura 5.15 (b), la scara $J=3$ rezultă și cele mai puține alarme false ($F_s=793$). Prin urmare, cea mai bună performanță P_s , este furnizată la scara $J=3$.

În cazul maximizării raportului $\frac{P_s}{F_s}$ și a mărimii $\frac{1}{2} \cdot DR_2 + \frac{1}{2} \cdot \frac{P_s}{F_s}$, avem rezultatele din figura 5.16 (a) și (b).

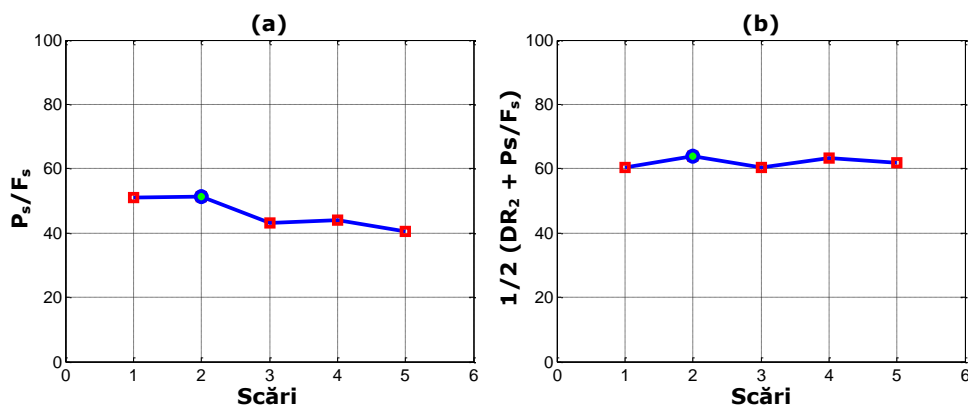


Figura 5.16. Performanțele P_s/F_s (a) și $1/2 (DR_2 + P_s/F_s)$ (b), pe cele 5 scări

Analizând cele două curbe din figura 5.16, se poate nota faptul că performanțele cele mai bune sunt obținute la scara $J=2$: $\frac{P_s}{F_s} = 51,18$ % și

$\frac{1}{2} \cdot DR_2 + \frac{1}{2} \cdot \frac{P_s}{F_s} = 64,01$ %. În plus, se constată o scădere a performanțelor $\frac{P_s}{F_s}$,

odată cu creșterea nivelului de descompunere. Anomaliile cu o durată mai scurtă decât rezoluția temporală corespunzătoare unui anumit nivel de descompunere sunt mai greu detectate la acel nivel. În consecință, odată cu creșterea nivelului de descompunere, scade capacitatea de detecție, deoarece anomaliile mai scurte decât rezoluția temporală corespunzătoare sunt mai greu de detectat. De exemplu anomalia 11 are durata de 1 minut, conform tabelului 5.2. Analizând tabelul 5.8 se constată că anomalia 11 a fost detectată o singură dată la rezoluția temporală de 32 de minute ($J=5$), în cazul semnalului M12, cu ajutorul criteriului C2, folosind undișoara mamă Daub-8. Analizând tabelul 5.7 se constată că anomalia 11 a fost detectată de 11 ori la rezoluția temporală de 16 minute ($J=4$), în cazul perechilor de semnale și criterii: M2 C2, M5 C2, M6 C2, M7 C2, M8 C2, M9 C2, M10 C2, M12 C2 și C3, M13 C2 și M14 C2. Deci anomalia 11 este mai greu de detectat la rezoluția de 32 de minute decât la rezoluția de 16 minute.

Până în acest moment, am efectuat o analiză detaliată a rezultatelor detecției furnizate de către metoda propusă, separat pe cele 5 scări. Am făcut, de asemenea și un studiu comparativ al performanțelor între aceste scări. Se urmărește, în continuare, punerea în evidență a efectelor corelării rezultatelor mai multor scări, asupra performanțelor globale de detecție. Din acest punct de vedere, credem că vor putea fi extrase concluzii foarte interesante.

Rezultatele obținute sunt redată în tabelul 5.9. Corelarea rezultatelor se face progresiv, ajungându-se în final la corelarea rezultatelor detecției de pe toate scările. Performanțele cele mai bune de detecție sunt marcate în tabel, prin intermediul unui fundal colorat.

J=1,2						
		P_S	F_S	P_S / F_S	DR_1 / Anomalii detectate	DR_2
Corelare M_i	C1	89	194	45.88	75/1,2,3,4,5,6,7,8,9,10,14,16	68.46
	C3	126	448	28.13	93.75/100/1,2,3,4,5,6,7,8,9,10,11,12,14,15,16	96.92
J=1,2,3						
		P_S	F_S	P_S / F_S	DR_1 / Anomalii detectate	DR_2
Corelare M_i	C1	105	251	41.83	87.5/1,2,3,4,5,6,7,8,9,10,12,14,15,16	80.76
	C3	126	514	24.51	93.75/1,2,3,4,5,6,7,8,9,10,11,12,14,15,16	96.92
J=1,2,3,4						
		P_S	F_S	P_S / F_S	DR_1 / Anomalii detectate	DR_2
Corelare M_i	C1	119	329	36.17	87.5/1,2,3,4,5,6,7,8,9,10,12,14,15,16	91.53
	C3	126	530	23.77	93.75/1,2,3,4,5,6,7,8,9,10,11,12,14,15,16	96.92
J=1,2,3,4,5						
		P_S	F_S	P_S / F_S	DR_1 / Anomalii detectate	DR_2
Corelare M_i	C1	120	423	28.37	87.5/1,2,3,4,5,6,7,8,9,10,12,14,15,16	92.30
	C3	128	649	19.72	100/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	98.46

Tabel 5.9. Performanțele de detecție ale anomaliilor obținute prin corelarea rezultatelor mai multor scări, pentru S4Z1

Într-adevăr, analiza rezultatelor din tabelul 5.9 dezvăluie câteva concluzii utile. Astfel, performanța F_S cea mai bună în aceste cazuri, este inferioară celei raportată anterior la scara 2. În ceea ce privește numărul maxim de eșantioane cu anomalii, sunt detectate un număr de 128 de eșantioane, la fel ca și în cazul scării 3, raportul $\frac{P_S}{F_S}$ având o valoare de 19,72 %, mai mare decât cea pentru scara 3 (16,14 %). Prin urmare, prin corelarea rezultatelor de pe toate scările considerate, se constată o îmbunătățire a performanței P_S . În schimb, performanțele $\frac{P_S}{F_S}$ și $\frac{1}{2} \cdot DR_2 + \frac{1}{2} \cdot \frac{P_S}{F_S}$ sunt inferioare performanțelor obținute la scara 2, corelarea neaducând nici o îmbunătățire a acestor performanțe.

În concluzie, prin corelarea rezultatelor diverselor scări se constată practic, cu o singură excepție, o degradare a performanțelor de detecție avute în vedere.

5.9.3. Alegerea undișoarei mamă

Există câteva familii de undișoare bine-cunoscute și utilizate adesea pentru calculul diferitelor transformări wavelet [Mal99]. Ne putem referi aici la undișoarele Haar, Daubechies, Coiflet și Symmlet. Toate aceste undișoare au avantajul că filtrele digitale cu ajutorul cărora se implementează algoritmul lui Mallat sunt cunoscute. Pentru toate aceste undișoare mai există un parametru de luat în calcul, și anume

numărul de momente nule al undișoarei mamă. În principiu, cu cât acest număr este mai mare cu atât undișoara mamă va fi mai întinsă în timp și mai concentrată în frecvență.

Se va trece în continuare la ilustrarea rezultatelor de simulare obținute și la discuții pe marginea acestora. Obiectivul principal al acestui paragraf este de a analiza modul cum tipul undișoarei mamă ales, afectează performanțele de detecție a metodei propuse. Simulările sunt efectuate la scara 1, iar familiile de undișoare considerate sunt cele prezentate în tabelul 5.3.

În tabelul 5.10 sunt prezentate performanțele de detecție obținute în cazul familiei de undișoare Daubechies. Din tabel reiese faptul că, utilizând undișoara Haar se obțin cele mai bune performanțe F_S și P_S , iar pentru $\frac{P_S}{F_S}$, utilizând undișoara

Daubechies-8. Maximizarea performanței $\frac{1}{2} \cdot DR_2 + \frac{1}{2} \cdot \frac{P_S}{F_S}$ este atinsă pentru undișoara Daubechies-6.

		ψ	P_S	F_S	P_S / F_S	DR_1 / Anomalii detectate	DR_2
Cor M_j	C1	Haar	67	147	45.58	50/1,3,6,7,8,10,14,16	51.53
		Daub-4	53	157	33.76	56.25/1,2,3,6,7,8,11,14,16	40.76
		Daub-6	68	161	42.24	68.75/1,2,3,4,6,7,8,10,11,14,16	52.30
		Daub-8	73	156	46.79	68.75/1,2,3,4,5,6,7,8,10,12,16	56.15
Cor M_j	C3	Haar	115	341	33.72	87.5/1,2,3,4,5,6,7,8,10,11,12,14,15,16	88.46
		Daub-4	106	254	41.73	81.25/1,2,3,4,5,6,7,8,11,12,14,15,16	81.53
		Daub-6	114	279	40.86	93.75/1,2,3,4,5,6,7,8,9,10,11,12,14,15	87.69
		Daub-8	113	333	33.93	87.5/1,2,3,4,5,6,7,8,10,11,12,14,15,16	86.92

Tabel 5.10. Performanțele de detecție ale anomaliilor pentru S4Z1, cu undișoarele Daubechies, la scara $J=1$

Performanțele rezultate pentru familia de undișoare Coiflet sunt ilustrate în tabelul 5.11.

		ψ	P_S	F_S	P_S / F_S	DR_1 / Anomalii detectate	DR_2
Cor M_j	C1	Coiflet-1	60	155	38.71	56.25/1,3,4,5,6,7,8,14,16	46.15
		Coiflet-2	62	170	36.47	62.5/1,2,3,6,7,8,10,11,14,16	47.69
		Coiflet-3	65	166	39.16	56.25/1,2,3,6,7,8,10,14,16	50
Cor M_j	C3	Coiflet-1	96	314	30.57	87.5/1,2,3,4,5,6,7,8,9,11,12,14,15,16	73.84
		Coiflet-2	109	305	35.74	81.25/1,2,3,4,5,6,7,8,10,11,12,14,15,16	83.84
		Coiflet-3	109	287	37.98	81.25/1,2,3,4,5,6,7,8,11,12,14,15,16	83.84

Tabel 5.11. Performanțele de detecție ale anomaliilor pentru S4Z1, cu undișoarele Coiflet, la scara $J=1$

Analizând rezultatele din tabelul 5.11, se observă că având în vedere criteriile de performanță P_S , $\frac{P_S}{F_S}$ și $\frac{1}{2} \cdot DR_2 + \frac{1}{2} \cdot \frac{P_S}{F_S}$, undișoara Coiflet-3 oferă cele mai bune rezultate. Cele mai puține alarme false se obțin utilizând undișoara Coiflet-1.

Pentru familia de undișoare Symmlet, rezultatele detecției sunt redată în tabelul 5.12. Pentru aceste tipuri de undișoară, cele mai bune performanțe sunt obținute în cazul undișoarei Symmlet-5 și Symmlet-6.

		ψ	P_S	F_S	P_S / F_S	$DR_1 /$ Anomalii detectate	DR_2
Cor M_i	C1	Symmlet-4	62	175	35.43	56.25/1,3,4,6,7,8,11,14,16	47.69
		Symmlet-5	66	164	40.24	56.25/1,2,3,6,7,8,10,14,16	50.76
		Symmlet-6	67	176	38.07	68.75/1,2,3,5,6,7,8,10,14,15,16	51.53
Cor M_i	C3	Symmlet-4	102	313	32.59	87.5/1,2,3,4,5,6,7,8,10,11,12,14,15,16	78.46
		Symmlet-5	95	302	31.46	68.75/1,2,6,7,8,10,11,12,14,15,16	73.07
		Symmlet-6	109	306	35.62	87.5/1,2,3,4,5,6,7,8,10,11,12,14,15,16	83.84

Tabel 5.12. Performanțele de detecție ale anomaliilor pentru S4Z1, cu undișoarele Symmlet, la scara $J=1$

Având în vedere rezultatele prezentate anterior, putem trage câteva concluzii importante. În primul rând, putem constata faptul că, cele mai bune performanțe sunt atinse pentru familia de undișoare Daubechies, urmate împreună de către familia de undișoare Coiflet și Symmlet. Mai mult, se pare că dintre undișoarele familiei Daubechies, undișoara Haar este cea mai adecvată în acest sens. De asemenea, observăm că prin utilizarea unei undișoare cu numărul cel mai mic de momente nule, se generează cele mai puține alarme false. Pe de altă parte, detecția unui număr mai ridicat de anomalii, necesită o undișoară mamă cu puțin mai multe momente nule, decât numărul minim posibil de momente nule. O altă observație importantă este aceea că, utilizând doar un singur tip de undișoară se obțin performanțe ceva mai slabe decât în cazul în care se folosește un număr mai mare de tipuri de undișoare mamă, situație studiată în paragraful 5.9.2.

5.9.4. Influența lungimii ferestrei de detecție

Se poate merge mai departe cu analiza, studiind influența lungimii ferestrei de detecție aleasă L_{det} , asupra performanțelor de detecție. Ca și în paragraful precedent, simulările sunt efectuate doar pentru scara 1. În tabelul 5.13 sunt prezentate rezultatele simulărilor.

5.9 – Analiza performanțelor de detecție a anomaliilor 101

		L_{det}	P_S	F_S	P_S / F_S	DR_1 / Anomalii detectate	DR_2
Cor M_j	C1	2	73	268	27.24	87.5/1,2,3,5,7,8,9,10,11,12,13,14,15,16	56.15
		8	71	168	42.62	75/1,3,4,5,6,7,8,10,12,14,15,16	54.61
		16	72	199	36.18	56.25/1,5,6,7,8,10,11,14,16	55.38
		32	54	244	22.13	50/1,6,7,8,9,11,14,16	41.53
Cor M_j	C3	2	101	381	26.51	100/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	77.69
		8	101	218	46.33	87.5/1,2,3,4,5,6,7,8,10,11,12,14,15,16	77.69
		16	114	294	38.78	81.25/1,2,3,4,5,6,7,8,10,11,12,14,15,16	87.69
		32	126	477	26.42	100/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	96.92

Tabel 5.13. Performanțele de detecție ale anomaliilor pentru S4Z1, pentru diferite lungimi L_{det} , la scara $J=1$

Din analiza rezultatelor din tabelul 5.13, se vede că pentru o fereastră cu o lungime de 8 minute, se obțin cele mai puține alarme false și cea mai bună performanță $\frac{P_S}{F_S}$, în timp ce pentru o fereastră cu o lungime mare, de 32 minute, se identifică cel mai mare număr de eşantioane cu anomalii.

5.9.5. Alegerea pragurilor de decizie

Se analizează, în cele ce urmează, performanțele sistemului de detecție a anomaliilor propus în figura 5.1, pentru diferite valori ale pragului de decizie. Pragurile de decizie considerate sunt $\lambda = a \cdot m_{CWC}$, cu $a=1,2,3$, unde m_{CWC} reprezintă media semnalului Cum4 obținut cu ajutorul ferestrei alunecătoare în timp, L_{det} , la scara 1. Performanțele detecției sunt redată în tabelul 5.14.

		a	P_S	F_S	P_S / F_S	DR_1 / Anomalii detectate	DR_2
Cor M_j	C1	1	128	845	15.15	100/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	98.46
		2	103	308	33.44	81.25/1,2,3,4,5,6,7,8,9,11,12,14,16	79.23
		3	67	139	48.20	68.75/1,2,3,4,5,6,7,8,10,14,16	51.53
Cor M_j	C3	1	128	860	14.88	100/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	98.46
		2	119	342	34.80	100/1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	91.53
		3	77	172	44.77	75/1,2,3,4,6,7,8,10,12,14,15,16	59.23

Tabel 5.14. Performanțele de detecție ale anomaliilor pentru S4Z1, pentru diferite praguri de decizie, la scara $J=1$

Rezultatele din tabelul 5.14 confirmă încă o dată concluziile din paragraful 5.9.2, și anume că, pentru un prag de valoare mică numărul anomaliilor detectate este foarte mare, iar numărul de alarme false la fel de mare, și că pentru un prag de

valoare mare, se obțin performanțele cele mai bune, în ceea ce privește compromisul care există între numărul de alarme pozitive și alarme negative.

5.10. Concluzii

Realitățile din ziua de azi, arată că odată cu creșterea exponențială a atacurilor/intruziunilor, este evident faptul că utilizarea doar a criptării și firewall-urilor nu pot asigura protejarea completă a calculatoarelor dintr-o rețea împotriva unor clase de comportamente malițioase. Așadar, este necesară dezvoltarea unei noi clase de aplicații de securitate, care să completeze tehnicile de protecție deja folosite. Aceste aplicații sunt numite sisteme de detecție a intruziunilor (IDS).

Astfel, obiectivul principal al capitolului 5 îl constituie proiectarea și dezvoltarea unui sistem de detecție a anomaliilor din traficul de rețea, cu o structură cât mai flexibilă, capabil să detecteze o gamă cât mai largă de atacuri. Rezultatele pe care le-am obținut în urma simulărilor, arată performanțe de detecție a anomaliilor foarte bune, superioare performanțelor raportate în [Wei09].

6. CONTRIBUȚII ȘI CONCLUZII

În acest capitol sunt prezentate contribuțiile originale cuprinse în lucrarea de față. Scopul urmărit în lucrare este dezvoltarea unor aplicații ale reprezentărilor timp-frecvență.

În paragraful 2.1.2 am propus o metodă pentru recunoașterea modulațiilor numerice mono-purtătoare și multi-purtătoare, ce utilizează o tehnică de filtrare cu o baterie de filtre ortogonale și reprezentarea timp-frecvență bazată pe modelarea polinomială a fazei semnalului, a cărei procedură de estimare a coeficienților polinomiali "WarpComp", este bazată pe operatori de deformare.

În paragraful 2.1.3 am analizat prin simulare, performanțele de separare a modulațiilor numerice. Rezultatele obținute, arată performanțe bune de detecție a purtătoarelor conținute în semnalele de test, metoda propusă constituind o soluție foarte bună pentru recunoașterea modulațiilor mono-purtătoare și multi-purtătoare. Rezultatele au fost publicate în [Sal04].

În paragraful 3.4 am efectuat un studiu al performanțelor metodei de prelucrare timp-frecvență ce utilizează operatori morfologici în estimarea frecvenței instantanee (TFR-MO). Am observat că pentru un semnal extrem de nestaționar, a cărui frecvență instantanee variază foarte rapid într-un interval scurt de timp, performanțele TFR-MO sunt inferioare metodelor WVD și CTD. Cu toate acestea, la rapoarte semnal pe zgomot mai mici de 4dB eroarea MSE pentru TFR-MO este mai mică decât erorile obținute în cazul celorlalte două metode analizate. În acest caz, prima concluzie care poate fi extrasă este că metoda TFR-MO este mai robustă la influența zgomotului. Pe de altă parte, pentru un semnal cu frecvența instantanee care variază mai lent, rezultatele de estimare cele mai bune se obțin pentru TFR-MO, atât pentru niveluri ridicate cât și pentru niveluri mici ale raportului semnal pe zgomot. Rezultatele obținute pentru acest tip de semnale demonstrează robustețea TFR-MO la rapoarte semnal pe zgomot mici. Rezultatele au fost publicate în [Sal07].

În paragraful 3.5 am propus o nouă implementare a metodei TFR-MO (TFR-IMO), bazată pe un algoritm secvențial de prelucrare, cu scopul de a îmbunătăți performanțele de estimare a metodei TFR-MO pentru semnale cu frecvența instantanee puternic neliniară. În urma simulărilor efectuate se constată o îmbunătățire semnificativă a performanțelor de estimare, erorile MSE reducându-se de aproximativ, două ori și jumătate comparativ cu performanțele TFR-MO. Rezultatele au fost publicate în [NS08].

În capitolul 4 am analizat un algoritm nou de determinare a celei mai bune undișoare mamă bazat pe teoria polinoamelor, care permite aproximarea cea mai bună a unui semnal, utilizând un număr minim de coeficienți wavelet.

În paragraful 4.2.1 am propus o metodă de estimare a ordinului unui polinom bazată pe strânsa legătură între teoria wavelet și teoria polinoamelor.

În paragraful 4.2.2 am efectuat o analiză riguroasă a performanțelor de aproximare a metodei propuse considerând o serie de semnale de test cu caracteristici variate. În urma simulărilor efectuate s-a constatat că pentru semnalele pentru care algoritmul a identificat cel puțin o undișoară cu coeficienți de detaliu nuli, folosind undișoara cu număr maxim de detalii nule, se obține eroarea de aproximare MSE cea mai mică și puterea conținută în coeficienții wavelet (de aproximare și de detaliu) cea mai mare. Rezultatele au fost publicate în [Sal09].

În paragraful 4.2.3 am studiat influența filtrării coeficienților wavelet de detaliu diferiți de zero. Astfel, am observat că prin eliminarea unui număr mai mic de coeficienți nenuli, refacerea semnalului inițial este foarte bună pentru toate undișoarele mamă folosite în simulări. În cazul unei filtrări a unui număr mare de detalii, energia concentrată în coeficienții rămași după filtrare este de asemenea într-un procent ridicat (de ordinul 99.99 %). Și în aceste cazuri, cele mai bune performanțe de aproximare se obțin pentru undișoara mamă care generează numărul cel mai mare de momente nule.

În paragraful 4.2.4 am analizat influența numărului de eșantioane din semnal asupra metodei propuse de selecție a undișoarelor mamă optime. Rezultatele obținute în acest caz conduc spre concluzia că, pentru analiza unor semnale cu un număr ridicat de variații rapide, ar fi necesar un număr mai mare de eșantioane din semnal. Acest lucru, oferă posibilitatea de a utiliza o undișoară mamă, a cărei coeficienți wavelet au cea mai bună concentrare a energiei semnalului.

În capitolul 5 am propus un sistem complet de detecție a anomaliilor de rețea, bazat pe transformarea wavelet staționară analitică (ASWT) și pe cumulantul de ordinul patru (Cum4) în algoritmul statistic de detecție.

În paragraful 5.8.1 am prezentat blocul de analiză a traficului de rețea din arhitectura generală a sistemului de detecție, care permite în același timp o stocare foarte flexibilă a fluxurilor de date și o caracterizare cât mai completă a trăsăturilor specifice ale traficului de rețea.

În paragraful 5.9.2 am efectuat o analiză a performanțelor de detecție a anomaliilor din traficul de rețea la diferite scări ale ASWT. Am constatat că pentru toate scările considerate sunt identificate în proporție de 100 %, toate tipurile de anomalii. Rata de detecție a eșantioanelor ce conțin anomalii este foarte mare, aceasta scăzând ușor, odată cu creșterea scării. Totuși, cele mai bune rezultate de detecție se obțin la scara 2. De asemenea, am efectuat și o analiză a performanțelor de detecție prin corelarea tuturor rezultatelor diverselor scări considerate. În acest caz, se constată o degradare a performanțelor de detecție, concluzia care poate fi extrasă este că pentru rezultate mai bune nu este recomandabilă corelarea rezultatelor detecției mai multor scări. Rezultatele au fost publicate în [SF10].

În paragraful 5.9.3 am arătat că undișoarele cu un suport temporal mai mic, deci mai bine localizate în timp conduc la generarea celor mai puține alarme false. Pe de altă parte, detecția unui număr mai ridicat de anomalii, necesită o undișoară mamă mai bine localizată în frecvență. Dintre toate undișoarele testate, undișoara Haar a condus, de departe, la obținerea celor mai bune rezultate.

În paragraful 5.9.4 am evaluat influența lungimii feretrei de detecție. Astfel, s-a constatat că, o fereastră de lungime mică oferă cel mai bun compromis în ceea ce privește detecția corectă a unui număr cât mai mare de eșantioane cu anomalii și generarea unui număr cât mai mic de alarme false, în timp ce o fereastră cu o lungime mai mare se obține cea mai mare rată de detecție.

În paragraful 5.9.5 am studiat modul în care alegerea pragurilor de decizie influențează performanțele de detecție ale anomaliilor din traficul de rețea. Rezultatele obținute confirmă încă o dată concluziile din paragraful 5.9.2, și anume că, pentru un prag de valoare mică numărul anomaliilor detectate este foarte mare, iar numărul de alarme false la fel de mare, și pentru un prag de valoare mare, se obțin performanțele optime, în ceea ce privește compromisul care există între numărul de alarme pozitive și alarme negative.

ANEXA 1

Pentru construcția operatorilor morfologici se utilizează niște mulțimi specifice, numite elemente structurante. În continuare elementul structurant se va nota cu K , unde $K = \{x \in R^n\}$. Simetrica acestei mulțimi notată cu \tilde{K} , este $\tilde{K} = \{-x \in R^n | x \in K\}$.

Operatorul de dilatare

O operație des utilizată în construcția operatorilor morfologici este diferența de tip Minkovski. Pentru două mulțimi A și K , aceasta se definește astfel:

$$A \div K = \{x \in R^n | K_x \subset A\}, \text{ unde } K_x = \{x+k | k \in K\} \quad (A1.1)$$

Alternativ, relația (A1.1) se poate scrie sub forma:

$$A \div K = \bigcap_{k \in \tilde{K}} A_k \quad (A1.2)$$

Pe baza relației de mai sus se poate exprima operatorul dual, numit adunarea de tip Minkovski:

$$A \oplus K = \bigcup_{k \in \tilde{K}} A_k \quad (A1.3)$$

Fiecare element ce aparține mulțimii $A \oplus K$, are proprietatea: $x \in \bigcup_{k \in \tilde{K}} A_k$.

Există prin urmare un k , astfel încât $x - k \in A$. Operația de adunare Minkovski a mulțimilor A și K , devine:

$$A \oplus K = \{u, \exists k \in K, u - k \in A\} \quad (A1.4)$$

Astfel, operatorul de dilatare a mulțimii A folosind elementul structurant K , este dat de adunarea de tip Minkovski a mulțimilor A și \tilde{K} :

$$A \oplus \tilde{K} = \{u, \exists k \in K, u + k \in A\} \quad (A1.5)$$

Deoarece condiția $u + k \in A$ este echivalentă cu condiția $K_u \subset A$, sau $K_u \cap A \neq \emptyset$, expresia dilatării (A1.5) se poate scrie:

$$A \oplus \tilde{K} = \{u, K_u \cap A \neq \emptyset\} \quad (A1.6)$$

Operatorul de scheletizare

Scheletul este o transformare mai complexă și este compusă din mai multe operații morfologice de bază.

Fie $B(x, r)$ sfera închisă, de centru x și raza r și $\overset{\circ}{B}(x, r)$ sfera deschisă corespunzătoare (interiorul sferei închise).

Definiție Fie G o mulțime din plan. Sfera deschisă $\overset{\circ}{B}(x, r)$ și închisă $B(x, r)$ este maximală în G dacă și numai dacă:

$$\left. \begin{array}{l} \overset{\circ}{B}(x,r) \subset \overset{\circ}{B}(x',r') \subset G \\ \text{sau} \\ B(x,r) \subset B(x',r') \subset G \end{array} \right\} \Leftrightarrow x = x', r = r' \quad (\text{A1.7})$$

Definiție Scheletul mulțimii G este locul geometric al centrelor sferelor deschise maximale în G .

Lantuéjoul [Lan78] în teza sa de doctorat a introdus o formulă de calcul al scheletului exprimată astfel:

$$Sq(G) = \bigcup_{r>0} \bigcap_{\varepsilon>0} \left[\left(G \div \overset{\circ}{B}(r) \right) \setminus \left(G \div \overset{\circ}{B}(r) \right)_{B(\varepsilon)} \right] \quad (\text{A1.8})$$

unde $G \div \overset{\circ}{B}(r)$ reprezintă o eroziune, iar $\left(G \div \overset{\circ}{B}(r) \right)_{B(\varepsilon)}$ reprezintă operatorul de

deschidere morfologică dintre mulțimea $G \div \overset{\circ}{B}(r)$ și sfera închisă $B(\varepsilon)$. Deschiderea morfologică se obține în urma unei operații de eroziune și a unei operații de dilatare.

ANEXA 2

Propoziția 1.

Pentru orice polinom de grad P , numărul cel mai mare de coeficienți de detaliu nuli ai DWT corespunzătoare este obținut atunci când este utilizată o undișoară mamă cu $P+1$ momente nule.

Demonstratie

Fie $\psi_p(t)$ undișoara mamă cu p momente nule: $\int_{-\infty}^{+\infty} t^k \psi_p(t) dt = 0$,

$k = \overline{0, p-1}$. Coeficienții de detaliu DWT, pentru un polinom $P(t)$ de gradul P în intervalul I sunt:

$$d_p[n] = \langle P(t), {}_p\psi_p(t-n) \rangle = \left\langle P(t), 2^{\frac{p}{2}} \psi_p(2^p t - n) \right\rangle \quad (\text{A2.1})$$

unde p reprezintă numărul de iterații ale transformatei wavelet discretă.

Polinomul $P(t)$ mai poate fi exprimat și sub forma:

$$P(t) = \sum_{k=0}^P a_k t^k, \text{ pentru } t \in I \quad (\text{A2.2})$$

Rezultă astfel, coeficienții de detaliu DWT la scara p :

$$d_p[n] = \sum a_k \left\langle t^k, 2^{\frac{p}{2}} \psi_p(2^p t - n) \right\rangle \quad (\text{A2.3})$$

unde t aparține intervalului $I = [m, M]$. Dar:

$$\begin{aligned} \left\langle t^k, 2^{\frac{p}{2}} \psi_p(2^p t - n) \right\rangle &= 2^{\frac{p}{2}} \int_m^M t^k \psi_p(2^p t - n) dt = \\ &= \sum_{o=0}^k C_k^o \left(\int_{2^p m - n}^{2^p M - n} v^o \psi_p(v) dv \right) n^{k-o} \end{aligned} \quad (\text{A2.4})$$

Există, prin urmare, trei situații posibile:

Cazul 1

Supportul undișoarei mamă $\psi_p(t)$, este inclus în intervalul

$I_{pm} = [2^p m - n, 2^p M - n]$, caz în care:

$$\int_{2^p m - n}^{2^p M - n} v^o \psi_p(v) dv = \int_{-\infty}^{+\infty} v^o \psi_p(v) dv \quad (\text{A2.5})$$

deoarece, $0 \leq k \leq P$ și undișoara mamă $\psi_p(t)$ are $P+1$ momente nule. Astfel, toți coeficienții de detaliu $d_p[n]$ sunt nuli, $d_p[n] = 0$.

Cazul 2

Supportul undișoarei mamă $\psi_p(t)$, nu este inclus în intervalul I_{pm} , dar intersecția lor nu este nulă. În această situație, coeficienții $d_p[n]$ nu sunt nuli, $d_p[n] \neq 0$.

Cazul 3

Intersecția suportului undișoarei mamă $\psi_p(t)$, cu intervalul I_{pm} este nulă. În acest caz, toți coeficienții de detaliu $d_p[n]$ sunt nuli, $d_p[n] = 0$.

Doar în cel de-al doilea caz există coeficienți de detaliu diferiți de zero. De asemenea, dacă se folosește o undișoara mamă cu mai puține momente nule, atunci și în primul caz câteva detalii vor fi diferite de zero. Dacă în schimb, se utilizează o undișoara mamă cu mai multe momente nule, atunci în primul și al treilea caz, coeficienții de detaliu rămân nuli. În ambele situații, numărul de coeficienți de detaliu diferiți de zero este mai mare decât în cazul undișoarei mamă cu $P+1$ momente nule. Acest fapt este valabil și pentru cazul al doilea. În concluzie, cel mai mic număr de coeficienți de detaliu nuli se obțin utilizându-se undișoara $\psi_p(t)$, cu $P+1$ momente nule.

BIBLIOGRAFIE

- [Porat93] B. Porat, *"Digital Processing of Random Signals"*, Prentice Hall, New Jersey, 1993.
- [Barb96] S. Barbarossa, A. Porchia, A. Scaglione, *"Multiplicative multilag higher-order ambiguity function"*, in Proc. Int. Conf. Acoustics, Speech and Signal Processing, vol.5, pp. 3022-3026, Atlanta, 1996.
- [Barb98] S. Barbarossa, A. Scaglione, G.B. Giannakis, *"Product High-Order Ambiguity Function for Multicomponent Polynomial-Phase Signal Modeling"*, IEEE Transactions on Signal Processing, vol. 46, No. 3, March 1998.
- [Ioana03] C. Ioana, *"Contribution à la Caractérisation des Structures Temps-Fréquence Non-Linéaires"*, Thèse de doctorat, ENSIETA, Septembre 2003.
- [Cornu06] C. Cornu, *"Extraction de signaux et Caractérisation des lois de phase instantanéé – Application aux modulations non linéaires"*, Thèse de doctorat, ENSIETA, Octobre 2006.
- [COMINT04] COMunication INTelligence, Laboratoire E3I2, ENSIETA, 2004.
- [Stank02] L.J. Stankovic, *"Time-frequency distributions with complex argument"*, IEEE Tran. On Signal Processing, vol. 50, no.3, pp. 475-486, March 2002.
- [Isar02] Dorina Isar, Alexandru Isar, *"A New Best Wavelet's Mother Searching Algorithm"*, Revue roumaine des sciences techniques, serie Électrotechn. et energetique, Tome 47, vol. 3, 2002.
- [Isar04] Dorina Isar, Alexandru Isar, *"Polynomial Approximation of Signals Corrupted by Noise"*, Proceedings of International Conference OPTIM'04, Brasov, vol.IV, pp. 153-158, 20-21 May, 2004.
- [Isar03] A. Isar, D. Isar, M. Bianu, *"Statistical Analysis of Two Classes of Time-Frequency Representations"*, Facta Universitatis, series Electronics and Energetic, vol. 16, no.1, Nis, Serbia, 115-134, April 2003.
- [Daub92] I. Daubechies, *"Ten Lectures on Wavelets"*, SIAM, Philadelphia 1992.
- [BNI05] Monica Borda, Ioan Naforntita, Dorina Isar, Alexandru Isar, *"New instantaneous frequency estimation method based on image processing techniques"*, Journal of Electronic Imaging, Vol. 14, Issue2, 023013_1-023013_11, April-June 2005.
- [Lan78] C. Lantuejoul, *"La squelettisation et son application aux mesures topologiques des mosaïques polycristallines"* these de Docteur-ingenieur, School of Mines, Paris, France, 1978.
- [Mal99] Stephane Mallat, *"A Wavelet Tour of Signal Processing"*, Academic Press, 1999.
- [Cohen95] L. Cohen , *"Time-Frequency Analysis"*, Prentice Hall, New Jersey, 1995.
- [Mal89] S. Mallat, *"Multiresolution Approximation and Wavelet Orthonormal Bases of $L_2(R)$ "*, Trans. Amer. Math. Soc., 315, pp.69-87, 1989.
- [Ches94] W. Cheswick, S. Bellovin, *"Firewalls and Internet Security"*, Addison-Wesley, Reading, Massachusetts, USA, 1994.
- [Land94] C. E. Landwehr, Bull A. R., McDermott J. P., Choi W. S., *"A Taxonomy of Computer Program Security Flaws. ACM Computing Surveys (CSUR)"*, 26(3):211–254, 1994.
- [CERT] CERT Statistics (Historical), <http://www.cert.org/stats/>.

- [Resco03] E. Rescorla, "Security holes... Who cares?", In Paxson, V., editor, USENIX Security Symposium, pages 75–90, USENIX, 2003.
- [Bello01] S. Bellovin, "Computer Security - An End State?", Communications of the ACM, 44(3):131–132, 2001.
- [Dacier99] Dacier M., Debar H., Wespi A., "Towards a taxonomy of intrusion-detection systems", Computer Networks, 31 (8):805–822, 1999.
- [Axel98] S. Axelsson, "Research in intrusion-detection systems: A survey", Department of Computer Engineering, Chalmers University of Technology, Goteborg, Sweden, Technical Report 98--17, December 1998.
- [Axel99] S. Axelsson, "The Base-Rate Fallacy and Its Implications for the Difficulty of Intrusion Detection", in ACM Conference on Computer and Communications Security, pages 1–7, 1998.
- [Stick04] "IDS stress tool", 2004, <http://www.eurocompton.net/stick/projects8.html>.
- [Snot04] "A packet generator", 2004, <http://www.stolenshoes.net/sniph/>.
- [Snort] <http://www.snort.org/snort>.
- [Kumar94] S. Kumar, E.H. Spafford, "An application of pattern matching in intrusion detection", The COAST Project, Department of Computer Sciences, Purdue University, West Lafayette, IN, USA, Technical Report CSD-TR-94-013, June 17, 1994.
- [Cheng02] C.-M. Cheng, H.T.Kung, K.-S. Tan, "Use of spectral analysis in defense against DoS attacks", IEEE GLOBECOM, pp. 2143-2148, 2002.
- [Lakhina04] A. Lakhina, M. Crovella, C. Diot, "Diagnosing Network-Wide Traffic Anomalies", ACM SIGCOMM 2004.
- [Gu05] Y. Gu, A. McCallum, D. Towsley, "Detecting Anomalies in Network Traffic Using Maximum Entropy Estimation", IMC 2005.
- [Siris04] V. A. Siris, F. Papagalou, "Application of Anomaly Detection Algorithms for Detecting SYN Flooding Attacks", IEEE GLOBECOM 2004, pp. 2050-2054, Nov. 2004.
- [Blazek01] R. B. Blazek, H. Kim, B. Rozovskii, A. Tartakovsky, "A Novel Approach to Detection of Denial-of-Service Attacks via Adaptive Sequential and Batch-Sequential Change-Point Detection Methods", IEEE Workshop Information Assurance and Security, pp. 220-226, 2001.
- [DARPA99] DARPA Intrusion Detection Evaluation, Lincoln Laboratory, Massachusetts Institute of Technology, Lexington, 1999, <http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/1999data.html>.
- [KDD99] KDD Cup 1999 Data, <http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html>.
- [Hugh00] J. McHugh, "Testing Intrusion detection systems: a critique of the 1998 and 1999 DARPA intrusion detection", ACM Transactions on Information and System Security 3, 262–294, 2000.
- [Haines99] Joshua W. Haines, Richard P. Lippmann, David J. Fried, Eushuan Tran, Steve Boswell, Marc A. Zissman, "1999 DARPA Intrusion Detection System Evaluation: Design and Procedures ", MIT Lincoln Laboratory Technical Report, 1999.
- [Barford02] P. Barford, J. Kline, D. Plonka, and A. Ron, "A signal analysis of network traffic anomalies", in Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement (IMW '02), pp. 71–82, Marseille, France, November 2002.

- [Raman02] A. Ramanarran, "WADES : a tool for distributed denial of service attack detection", M.S. thesis, Texas A&M University, College Station, Tex, USA TAMU-ECE, 2002.
- [Kim05] Seong Soo Kim, "Real-time Analysis of Aggregate Network Traffic for Anomaly Detection", Dissertation, Texas A&M University, May 2005.
- [Huang06] C.-T. Huang, S. Thareja, Y.-J. Shin, "Wavelet-based real time detection of network traffic anomalies", in Proceedings of Workshop on Enterprise Network Security and the 2nd International Conference on Security and Privacy in Communication Networks, pp. 1-7, Baltimore, Md, USA, August 2006..
- [Dainotti06] A. Dainotti, A. Pescapé, and G. Ventre, "Wavelet-based detection of DoS attacks", in Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '06), pp. 1-6, San Francisco, Calif, USA, November 2006.
- [Chang06] J.Gao, G. Hu,X. Yao, R. K. C. Chang, "Anomaly detection of network traffic based on wavelet packet", in Proceedings of the Asia-Pacific Conference on Communications (APCC '06), pp. 1-5, Busan, Korea, August 2006.
- [Wei09] Wei Lu, Ali A. Ghorbani, "Network Anomaly Detection Based on Wavelet Analysis", EURASIP Journal on Advances in Signal Processing, vol. 2009, Article ID 837601, 16 pages, 2009.
- [FIB09] Ioana Firoiu, Alexandru Isar, Jean-Marc Boucher, "An Improved Version of the Inverse Hyperanalytic Wavelet Transform", Proceedings of IEEE International Symposium SCS'09, Iași, Romania, ISBN 1-4244-0968-3, 13-16, July 9-10, 2009.
- [Tcpcap] Tcpcap/Libpcap public repository, <http://www.tcpcap.org/>.
- [AOB06] I. Adam, M. Oltean, M. Bora, "A New Quasi Shift Invariant Non-Redundant Complex Wavelet Transform", Scientific Bulletin of the "POLITEHNICA" University of Timisoara, number dedicated to the Symposium on Electronics and Telecommunications ETC 2006 7th Edition, Timisoara, Tom 51 (65), Fascicola 2, 2006 ISSN 1583-3380, pp.14-18, September 2006.
- [Mallat99] S. Mallat, "A Wavelet Tour of Signal Processing", 2nd edition, Academic Press, New York, 1999.
- [LGOBW96] M. Lang, H. Guo, J.E. Odegard, C.S. Burrus and R.O. Wells Jr., "Noise reduction using an undecimated wavelet transform", IEEE Signal Processing Letters, vol. 3, no. 1, pp. 10 - 12, Jan. 1996.
- [Abry94] P. Abry, "Transformées en ondelettes-Analyses multirésolution et signaux de pression en turbulence", Ph.D. dissertation, Université Claude Bernard, Lyon, France, 1994.
- [King99] N. G. Kingsbury, "Image Processing with Complex Wavelets", Philosophical Transactions of the Royal Society of London A, vol. 357, pp. 2543 - 2560, 1999.
- [King01] N. G. Kingsbury, "Complex wavelets for shift invariant analysis and filtering of signals", Journal of Applied and Computational Harmonic Analysis, vol. 10, no. 3, pp. 234 - 253, May 2001
- [FIB09] Ioana Firoiu, Alexandru Isar, Jean-Marc Boucher, "An Improved Version of the Inverse Hyperanalytic Wavelet Transform," Proceedings of IEEE International Symposium SCS'09, Iași, Romania, ISBN 1-4244-0968-3, 13-16, July 9-10, 2009.
- [Sal04]** Marius Salagean, Cornel Ioana, Andre Quinquis, "Recognition of OFDM modulations : approach based on high-order time-frequency methods", Buletinul Științific al Universității „Politehnica” Timișoara, Seria Electronică și Telecomunicații, Tom 49-63, Fascicola 2, 2004.
- [Sal09]** Marius Salagean, "On the polynomial approximation", International Symposium on Signal, Circuits and Systems, ISSCS 2009, Iasi, Romania, 09-10 July, 2009.

- [Sal07]** Marius Salagean, *"The Use of the Improved Time-Frequency Method Based on Mathematical Morphology Operators"*, Buletinul Științific al Universității „Politehnica” Timișoara, Seria Electronică și Telecomunicații, Tom 52 (66), ISSN 1583-3380, Fascicola 2, pp. 45-49, 2007.
- [NS07]** Marius Salagean, Nafornta Ioan, *"Improved Time-Frequency Method Based on Mathematical Morphology Operators"*, Lucrarile Sesiunii de Comunicari Stiintifice Doctor Etc 2007, Timisoara, pp. 10-13, ISBN: 978-973-625-494-9, Septembrie 2007.
- [NS08]** Marius Salagean, Nafornta Ioan, *"A New Processing Algorithm For the Time-Frequency Mathematical Morphology Operators Method"*, Buletinul Științific al Universității „Politehnica” Timișoara, Seria Electronică și Telecomunicații, Tom 53 (67), ISSN 1583-3380, Fascicola 2, pp. 198-202, 2008.
- [SF10]** Marius Salagean, Ioana Firoiu, *"Anomaly Detection of Network Traffic Based on Analytical Discrete Wavelet Transform"*, International Conference on Communications, Volume 1, 49-52, Bucharest, Romania, 10-12 June, 2010.
- [Salagean10]** Marius Salagean, *"Real Network Traffic Anomaly Detection Based on Analytical Discrete Wavelet Transform"*, International Conference on Optimization of Electrical and Electronic Equipment, Brasov, Romania, 20-22 May, 2010.
- [Sal02]** Marius Salagean, Mirela Bianu, Cornelia Gordan, *"Instantaneous Frequency and its Determination"*, Buletinul Științific al Universității „Politehnica” Timișoara, Seria Electronică și Telecomunicații, Tom 47(6), 2002.
- [Sal06]** Marius Salagean, Ioan Nafornta, *"The estimation of the instantaneous frequency using time-frequency methods"*, Buletinul Științific al Universității „Politehnica” Timișoara, Seria Electronică și Telecomunicații, Tom 51 (65), ISSN 1583-3380, Fascicola 2, pp. 195-198, 2006.
- [Sala07]** Marius Salagean, Ioan Nafornta, *"Time-frequency methods for multicomponents signals"*, International Symposium on Signal, Circuits and Systems, ISSCS 2007, Iasi, Romania, 12-13 July 2007.
- [GSBN02]** Janos Gal, Marius Salagean, Mirela Bianu, Ioan Nafornta, *"The Instantaneous Frequency Determination for Signals with Polynomial Phase using Kalman Filtering"*, Buletinul Științific al Universității „Politehnica” Timișoara, Seria Electronică și Telecomunicații, Tom 47(6), 2002.
- [NSOS03]** Elena Lupea, Mirela Bianu, Marius Oltean, Marius Salagean, Miranda Nafornta, *"BER Performance of Frequency Selective Channels with Cyclic Prefix Base Equalisers"*, Buletinul Științific al Universității „Politehnica” Timișoara, Seria Electronică și Telecomunicații, Tom 48-62, Fascicola 2, 2003.
- [SM06]** Marius Salagean, Miranda Nafornta, *"Some Routing Trends"*, Analele Universitatii din Oradea, Fascicula Electrotehnica, Sectiunea Electronica, pp. 98-102, ISSN 1454-9239, 2006.