Univerzitet Crne Gore
Elektrotehnički fakultet

Anja Brtan

DETEKCIJA PROMJENE FUNKCIJE GUSTINE VJEROVATNOĆE SIGNALA SA PRIMJENOM NA IDENTIFIKACIJU GPS *SPOOFING* NAPADA NA UREĐAJE ZA SINHRONIZOVANO MJERENJE FAZORA

– MAGISTARSKI RAD –

Podgorica, 2025. godine

PODACI I INFORMACIJE O STUDENTU

Ime i prezime: **Anja Brtan**
Datum i mjesto rođenja: **20. jul 1999. godine, Podgorica**
Naziv završenog osnovnog studijskog programa i godina završetka studija: **Elektronika, telekomunikacije i računari, 2018. godine**

INFORMACIJE O MASTER RADU

Naziv master studija: **Postdiplomske akademske studije, odsjek Elektronika, telekomunikacije i računari, smjer Računari**
Naslov rada: **Detekcija promjene funkcije gustine vjerovatnoće signala sa primjenom na identifikaciju GPS *spoofing* napada na uređaje za sinhronizovano mjerenje fazora**
Fakultet na kojem je rad odbranjen: **Elektrotehnički fakultet Podgorica**

UDK, OCJENA I ODBRANA MASTER RADA

Datum prijave master rada: **1. jul 2024. godine**
Datum sjednice Vijeća na kojoj je prihvaćena tema i mentor: **24. oktobar 2024. godine**
Mentor: **Prof. dr Vesna Popović-Bugarin**
Komisija za ocjenu/odbranu rada:

1. **Prof. dr Vladan Radulović, ETF Podgorica, predsjednik**
2. **Prof. dr Vesna Popović - Bugarin, ETF Podgorica, mentor**
3. **dr Nenad Mijatović, Alstom Signaling LLC, Melbourne, Florida, USA, član**

Datum odbrane: **23. decembar 2025. godine**

Izjava o autorstvu

Potpisani-a Anja Brtan

Broj indeksa/upisa 7/21

Izjavljujem

da je master rad pod nazivom

"Detekcija promjene funkcije gustine vjerovatnoće signala sa primjenom na identifikaciju GPS *spoofing* napada na uređaje za sinhronizovano mjerenje fazora"

- rezultat sopstvenog istraživačkog rada,
- da predloženi master rad ni u cjelini ni u djelovima nije bio predložen za dobijanje bilo koje diplome prema studijskim programima drugih ustanova visokog obrazovanja,
- da su rezultati korektno navedeni, i
- da nijesam povrijedio/la autorska i druga prava intelektualne svojine koja pripadaju trećim licima.

U Podgorici, 25.11.2025. godine

Potpis magistranda

Anja Brtan

Predgovor

Ovaj master rad nastao je kao rezultat mog dosadašnjeg naučnog i profesionalnog interesovanja u oblasti digitalne obrade signala. Cilj rada je da predstavi korišćenje statističke metode za detekciju promjene funkcije gustine vjerovatnoće signala u svrhu identifikacije sajber napada na djelove elektroenergetskog sistema i prikaže rezultate do kojih sam došla kroz istraživanje, eksperimentisanje i teorijsku razradu problema.

Proces izrade ovog rada obuhvatio je detaljno proučavanje relevantne literature, implementaciju i testiranje metoda u oblasti energetike, kao i kritičku analizu dobijenih rezultata. Poseban izazov predstavljalo je istraživanje oblasti GPS *spoofing* napada kao i primjena same statističke metode na takavu vrstu problema, što je značajno doprinijelo produbljivanju mog razumijevanja ove oblasti.

Zahvalnost dugujem mentorki Prof. dr Vesni Popović-Bugarin na pruženoj podršci, stručnim savjetima i vremenu koje mi je posvetila pri izradi ovog rada. Takođe, želim da se zahvalim porodici, prijateljima i kolegama na podsticaju i razumijevanju tokom ovog procesa.

Nadam se da će rezultati prikazani u ovom radu doprinijeti daljem razvoju i boljem razumijevanju ove teme, te i poslužiti kao osnova za buduća istraživanja.

Sažetak

Detekcija promjene funkcije gustine vjerovatnoće signala ima široku primjenu u različitim industrijskim sektorima. Naučnoj zajednici su poznate mnoge parametarske i neparametarske metode detekcije promjene funkcije gustine vjerovatnoće, a u ovom radu opisana je neparametarska metoda koja detekciju vrši računanjem $L2$ norme između koeficijenata razvoja *Wavelet* distribucije različitih djelova signala.

Ova metoda detekcije primijenjena je na identifikaciju GPS *spoofing* napada (eng. *GPS Spoofing Attacks*) na jedinice za sinhronizovano mjerenje fazora (eng. *Phasor Measurement Units - PMUs*).

Jedinice za sinhronizovano mjerenje fazora koriste estimatore stanja koji prate vrijednosti naponskih i strujnih fazora različitih djelova elektroenergetskog sistema i time predstavljaju jednu od ključnih komponenti savremenih sistema za monitoring i zaštitu elektroenergetskih sistema.

Međutim, ovi uređaji za svoj rad koriste civilni GPS sat koji ne zahtijeva autentifikaciju, pa su podložne GPS *spoofing* napadima koji podrazumijevaju generisanje lažnog GPS signala u blizini GPS prijemnika i time navode estimatore stanja u jedinicama za sinhronizovano mjerenje fazora na praćenje lažnog GPS signala. S obzirom na ključnu ulogu pomenutih estimatora stanja u svim funkcijama upravljanja u realnom vremenu, blagovremena detekcija ovih napada predstavlja preduslov očuvanja sigurnosti pogona elektroenergetskih sistema.

Prilikom GPS *spoofing* napada unosi se fazni pomak u fazorska mjerenja struja i napona i time utiče na promjenu funkcije gustine vjerovatnoće signala ovih mjerenja, te se za njihovu detekciju mogu koristiti i statističke metode kakav je i metod detekcije promjene funkcije gustine vjerovatnoće signala koji je opisan u ovom radu.

Računanjem $L2$ norme između koeficijenata *Wavelet* distribucije analiziranog signala može se na jednostavan način detektovati momenat promjene njegove funkcije gustine vjerovatnoće i samim tim početak GPS *spoofing* napada. Zahvaljujući svojoj jednostavnosti, metod ne zahtijeva kompleksne hardverske komponente niti izrazite memorijske resurse, te je pogodan za implementaciju u realnim elektroenergetskim sistemima sa ograničenim resursima.

Ključne riječi: Wavelet transformacija, funkcija gustine vjerovatnoće signala, jedinice za sinhronizovano mjerenje fazora, GPS *spoofing* napadi, $L2$ norma

Abstract

Change point detection in random signal's probability density function (PDF) has wide applications across various industrial sectors. Numerous parametric and nonparametric methods for detecting changes in the PDF are well-established within the scientific community. This study presents a nonparametric approach that identifies changes by computing the $L2$ norm between wavelet coefficients derived from different segments of the signal's distribution.

The proposed detection method is applied to identify GPS spoofing attacks on Phasor Measurement Units (PMUs). PMUs utilize state estimators to monitor voltage and current phasors across different parts of the power system, serving as critical components in modern power system monitoring and protection frameworks.

However, these devices rely on civilian GPS signals that lack authentication mechanisms, rendering them susceptible to GPS spoofing attacks. Such attacks involve generating counterfeit GPS signals near the receiver, leading PMU state estimators to synchronize with false timing information. Given the pivotal role of state estimators in real-time grid management, timely detection from these attacks is essential to maintain the operational security of power systems.

GPS spoofing attacks introduce phase shifts in voltage and current phasor measurements, thereby altering the statistical properties of the signal. Consequently, statistical methods, such as the one described in this study, can be employed to detect these anomalies. By calculating the $L2$ norm between Wavelet coefficients of different signal segments, the method effectively identifies the onset of changes in the PDF, signaling potential GPS spoofing incidents.

Owing to its simplicity, the method does not necesseraly need complex hardware components or substantial memory resources, making it suitable for implementation in real-world power systems with limited computational capabilities.

Keywords: Wavalet transformation, probability density function, Phasor Measurement Units, GPS Spoofing Attacks, $L2$ norm

Sadržaj

1 Uvod

Detekcija promjene funkcije gustine vjerovatnoće signala predstavlja značajnu metodu u analizi slučajnih signala, posebno u kontekstu detekcije anomalija, promjene režima rada sistema i otkrivanja sajber napada. Pruža napredan statistički pristup za identifikaciju promjena u distribuciji podataka, što je korisno u aplikacijama koje zahtijevaju visoku osjetljivost na promjene u ponašanju signala. Detekcija promjene funkcije gustine vjerovatnoće signala se može vršiti parametarskim i neparametarskim metodama, [1].

Parametarske metode podrazumijevaju pretpostavljanje oblika funkcije gustine vjerovatnoće signala, odnosno modela distribucije i procjena njenih parametara. Kako bi se ova procjena mogla realizovati, potrebno je poznavati cijeli signal, odnosno sve njegove odbirke. Ove metode se zbog toga često u literaturi još nazivaju i *posteriori* metode za detekciju promjene funkcije gustine vjerovatnoće signala. Neke od ovih metoda zasnivaju se na mjeri maksimalne vjerovatnoće (eng. *Maximum Likelihood Estimation - MLE*), [2]. Ovakve metode koriste mjeru maksimalne vjerovatnoće za pronalaženje parametara koji maksimizuju funkciju vjerovatnoće. Još jedna od poznatijih parametarskih metoda je i računanje entropije između distribucija signala u dva različita vremenska intervala, [3]. Pored entropije, često se koristi i aproksimacija Kullback-Leibler divergencije. Budući da ona u opštem slučaju nema zatvorenu formu, u radu [4] je opisano nekoliko metoda njene aproksimacije. Pored jednodimenzionih podataka, analizirana je i obrada višedimenzionih podataka. Jedan od takvih pristupa je opisan u [5]. U tu svrhu se koriste statistički testovi za detekciju tačaka promjene statistike signala, a nakon toga se vrši procjena parametara statističkog modela signala unutar svakog od dobijenih segmenata.

Uprkos postojanju mnogih parametarskih metoda, pažnju privlače neparametarske metode procjene funkcije gustine vjerovatnoće signala zbog svoje fleksibilnosti i mogućnosti primjene na nepoznate signale sa kompleksnim statističkim karakteristikama što ih čini pogodnim za analizu signala u realnom vremenu. Ove metode se koriste i za detekciju promjene funkcije gustine vjerovatnoće signala, a većina njih se zasniva na poređenju statističkih osobina signala u dva različita vremenska intervala. Time omogućavaju detekciju promjena ovih statističkih osobina u realnom vremenu. Jedan od metoda detekcije promjene funkcije gustine vjerovatnoće signala je metoda detekcije korišćenjem estimacije jezgrima (eng. *kernel density estimation*), [6]. U ovom pristupu se vrši estimacija funkcija gustine vjerovatnoće signala unutar jezgara i njihovo međusobno poređenje mjerama udaljenosti između tih estimacija. Pomenute neparametarske metode podrazumijevaju procjenu funkcije gustine vje-

rovatnoće signala unutar vremenskih prozora pri analizi signala, a zatim računanje neke mjere udaljenosti, odnosno razlike, između ovih estimacija.

Metod detekcije promjene funkcije gustine vjerovatnoće signala koji se u ovom radu primjenjuje na identifikaciju GPS *spoofing* napada, opisan u [7], takođe analizira signal korišćenjem vremenskih prozora. Međutim, za razliku od prethodno opisanih neparametarskih metoda detekcije promjene funkcije gustine vjerovatnoće signala, ovaj metod ne zahtjeva estimaciju same funkcije gustine vjerovatnoće signala u analiziranim djelovima signala, već se u realnom vremenu računa $L2$ mjera između koeficijenata razvoja *Wavelet* distribucije signala u dva vremenska intervala obuhvaćena prozorima. U svrhu detekcije promjene funkcije gustine vjerovatnoće signala, u jednom koraku, sa svakim novim odbirkom koji se analizira vremenskim prozorima koji se pomjeraju, estimiraju se *Wavelet* koeficijenti razvoja distribucije korišćenjem *Garcia-Treviño* metoda, [8], i računa $L2$ mjera između koeficijenata estimiranih u dva vremenska prozora. Samim tim, ovaj metod omogućava pravovremenu detekciju anomalija signala i može se primijeniti na identifikaciju sajber napada na elektroenergetske sisteme kao što su GPS *spoofing* napadi koji mogu dovesti do katastrofalnih posljedica.

GPS *spoofing* napadi na jedinice (uređaje) za sinhronizovano mjerenje fazora (eng. *Phase Measurement Units* - PMU) se izdvajaju u odnosu na druge sajber napade zbog toga što se mogu jeftino realizovati korišćenjem osnovnih elektronskih komponenti i zbog toga predstavljaju posebnu vrstu prijetnje po eleketroenergetske sisteme.

Najpoznatiji sajber napad na elektroenergetski sistem, izveden na ukrajinski elektroenergetski sistem u decembru 2015. godine. Tokom ovog incidenta kompromitovani su sistemi za nadzor i upravljanje SCADA (eng. *Supervisory Control and Data Acquisition*) i ICS (eng. *Industrial Control Systems*), što je dovelo do onemogućavanja daljinskog upravljanja i prekida isporuke električne energije za oko 225.000 potrošača. Napad je uključivao više komponenti, kao što su ciljani fišing napad (eng. *Spear-Phishing Attacks*), korišćenje malvera (eng. *malware*), zloupotrebu legitimnih korisničkih naloga i brisanje sistemskih podataka. Posljedica ovog napada bila je onemogućavanje operativne kontrole i neovlašćena manipulacija uređajima na terenu, čime je potvrđena mogućnost prelaska sajber napada iz informacionog u fizički domen rada elektroenergetskih sistema.

Istraživanja u domenu rješavanja problema GPS *spoofing* napada se pretežno dijele ne dvije velike oblasti: metode detekcije GPS *spoofing* napada, [9–12] i metode korekcije napadnutog signala nakon detekcije, [10],[13–15].

Jedan od metoda detekcije napada je ispitivanje perturbacijama (eng. *probing*)

radi pronalaženja lokacije napadnute jedinice za sinhronizovano mjerenje fazora, [16]. Ovaj metod podrazumijeva prikupljanje informacija o faznim mjerenjima sa jedinica za sinhronizovano mjerenje fazora, računanje reziduala, odnosno, razlika između stvarnih mjerenja i predviđenih mjerenja dobijenih perturbacijama faznog ugla, i identifikovanje anomalija u ovim mjerenjima. Ovaj metod je pokazao dobre rezultate u pogledu brzine izvršavanja i greške estimacije, a razmatrana je i mogućnost umanjenja efekata GPS *spoofing* napada na ove signale.

U [17] je predstavljen još jedan metod za detekciju napada na jedinice za sinhronizovano mjerenje fazora koji detektuje napad na osnovu informacije o poziciji određene jedinice. Metod se oslanja na fiksne lokacije jedinica za sinhronizovano mjerenje fazora u elektroenergetskom sistemu i poređenje odstupanja GPS vremenske oznake jedne jedinice u odnosu na jedinice koje se nalaze u njenoj neposrednoj blizini. Na osnovu ovog odstupanja se tehnikom multilateracije, odnosno, određivanja lokacije izvora signala na osnovu razlika u vremenu njegovog dolaska do prijemnika, može lokalizovati jedinica sa GPS *spoofing* napadom. S obzirom na to da se metod oslanja na međusobnu vremensku usklađenost jedinica za sinhronizovano mjerenje fazora, autori zaključuju da je za ovaj metod potrebno minimalno pet međusobno vremenski usklađenih jedinica, ili šest međusobno vremenski neusklađenih jedinica.

U [18] je korišćen metod zasnovan na hipotetičkom testu koji analizira spektralnu gustinu snage signala unutar dva takozvana GPS prozora koji se dobijaju kombinacijom više GPS signala dobijenih u određenom vremenskom intervalu, a u cilju određivanja njihove međusobne korelacije. Ukoliko se utvrdi da analizirani djelovi signala međusobno nisu korelisani smatra se da je došlo do GPS *spoofing* napada. Eksperimentalno je utvrđeno da u realnim uslovima ovaj algoritam detektuje napade sa prosječnom tačnošću većom od 90%, te i da u slučaju greške u detekciji, odnosno kasne detekcije, ovo kašnjenje nije veće od 10 mikrosekundi.

Pored pomenutih metoda koje se zasnivaju na matematičkim modelima ili hardverskim rješenjima pojavljuju se i algoritmi detekcije GPS *spoofing* napada zasnovani na mašinskom učenju i vještačkoj inteligenciji, koji obuhvataju i neuralne mreže.

U [19] se koristi model sastavljen od bidirekcionog modela dugoročnog i kratkoročnog pamćenja (eng. *Long-Short Term Memory Model*) i transformera za detekciju GPS *spoofing* napada. Predloženi metod pokazuje naročito dobre rezultate, čak i u situacijama kada se napadi izvode na sistemima sa visokom penetracijom varijabilnih obnovljivih izvora energije, kao što su vjetroelektrane ili solarni paneli.

S obzirom na to da prilikom GPS *spoofing* napada dolazi do promjene faznog stava struje i napona i pojave faznog pomaka na svim mjerenjima jedinica za sin-

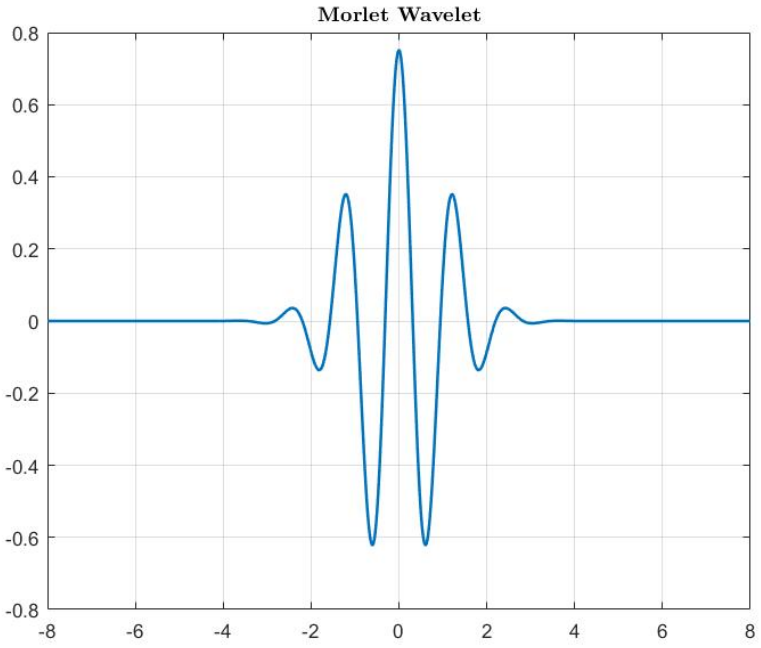
hronizovano mjerenje fazora pogođenih napadom, istovremeno dolazi do promjene funkcije gustine vjerovatnoće signala, sačinjenog od ovih fazorska mjerenja. Uzimajući u obzir ovakve posljedice, moguće je vršiti detekciju GPS *spoofing* napada korišćenjem statističkog metoda za detekciju funkcije gustine vjerovatnoće signala.

Ovaj rad opisuje primjenu metoda detekcije promjene funkcije gustine vjerovatnoće signala na identifikaciju GPS *spoofing* napada, i struktuiran je u šest poglavlja. U poglavlju 2 je dat teorijski opis *Wavelet* transformacije koja se koristi u detekciji promjene funkcije gustine vjerovatnoće signala, a u poglavlju 3 pregled metode čija se primjena istražuje. U sekciji 4 opisan je problem GPS *spoofing* napada na kom će metod biti primijenjen, dok je primjena same metode na detekciju GPS *spoofing* napada opisana u sekciji 5. Konačno, eksperimentalne metodologije i rezultati eksperimenata prikazani su u poglavlju 6.

Budući da su signali na jedinicama za sinhronizovano mjerenje fazora slučajni signali, u kojima prilikom GPS *spoofing* napada dolazi do naglih promjena distribucije različitog intenziteta, metodom detekcije promjene distribucije signala računanjem $L2$ norme između *Wavelet* koeficijenata moguće je brzo i precizno detektovati napade, čak i prilikom malih vrijednosti faznih pomaka koje izazivaju GPS *spoofing* napadi. Primjena metoda detekcije promjene funkcije gustine vjerovatnoće na identifikaciju GPS *spoofing* napada prestavlja memorijski efikasno rješenje, koje ne zahtijeva korišćenje snažnih procesorskih jedinica kao ni upotrebu velike količine podataka kao štoje to slučaj pri korišćenju modela mašinskog učenja. Takođe, ovakav pristup obezbjeđuje efikasnu detekciju GPS *spoofing* napada koja se zasniva na promjeni jedne od statističkih osobina signala, te ne zavisi od topologije elektrodistributivne mreže.

2 *Wavelet* transformacija

Wavelet transformacija je napredna tehnika za analizu digitalnog signala. Za razliku od tradicionalnih metoda, poput Furijeove transformacije, omogućava analizu signala kako u vremenskom, tako i u frekvencijskom domenu, uz zadržavanje lokalizacije u oba domena. Nasuprot drugim metodama koje koriste prozore konstantne širine, koristi funkcije prozora talasastog oblika, po kojima je i dobila ime (eng. *wavelet* - talasić). Ove činjenice omogućavaju korišćenje *Wavelet* transformacije u cilju detekcije promjene funkcije gustine vjerovatnoće signala. Prvi uvedeni oblik *Wavelet* transformacije je *Morlet Wavelet*, a naziv je dobila po francuskom geofizičaru *Jean*-u *Morlet*-u (1931-2007) koji ju je uveo u svoja istraživanja seizmičkih signala 1980. godine, [20]. Primjer *Morlet Wavelet* funkcije prozora je prikazan na slici 1.



Slika 1: Morlet Wavelet - prozor u *Wavelet* transformaciji

Wavelet transformacija omogućava istovremenu analizu komponenti signala na različitim frekvencijama sa različitim rezolucijama i time obezbjeđuje kvalitetniju obradu detalja, kao i detekciju malih i naglih promjena signala.

Prilikom analize signala korišćenjem *Wavelet* transformacije, koristi se matična *Wavelet* funkcija (eng. *mother Wavelet* funkcija, ϕ), koja predstavlja osnovni oblik *Wavelet* funkcije prozora za analizu signala. Matična *Wavelet* funkcija prozora se transformiše pomoću dvije osnovne operacije:

1. Translacija, koja se koristi za pomjeranje funkcije duž vremenske ose, omogućavajući analizu signala u različitim vremenskim trenucima.

2. Dilatacija, koja se koristi za skaliranje funkcije, širenje ili skupljanje, čime se omogućava analiza signala na različitim frekvencijskim opsezima.

Oblik *Wavelet* funkcije prozora koja se dobija primjenom ovih operacija na matičnu *Wavelet* funkciju prozora se u literaturi još naziva i skalirana *Wavelet* funkcija prozora (eng. *scaling Wavelet function* ili *father Wavelet function*) (ψ).

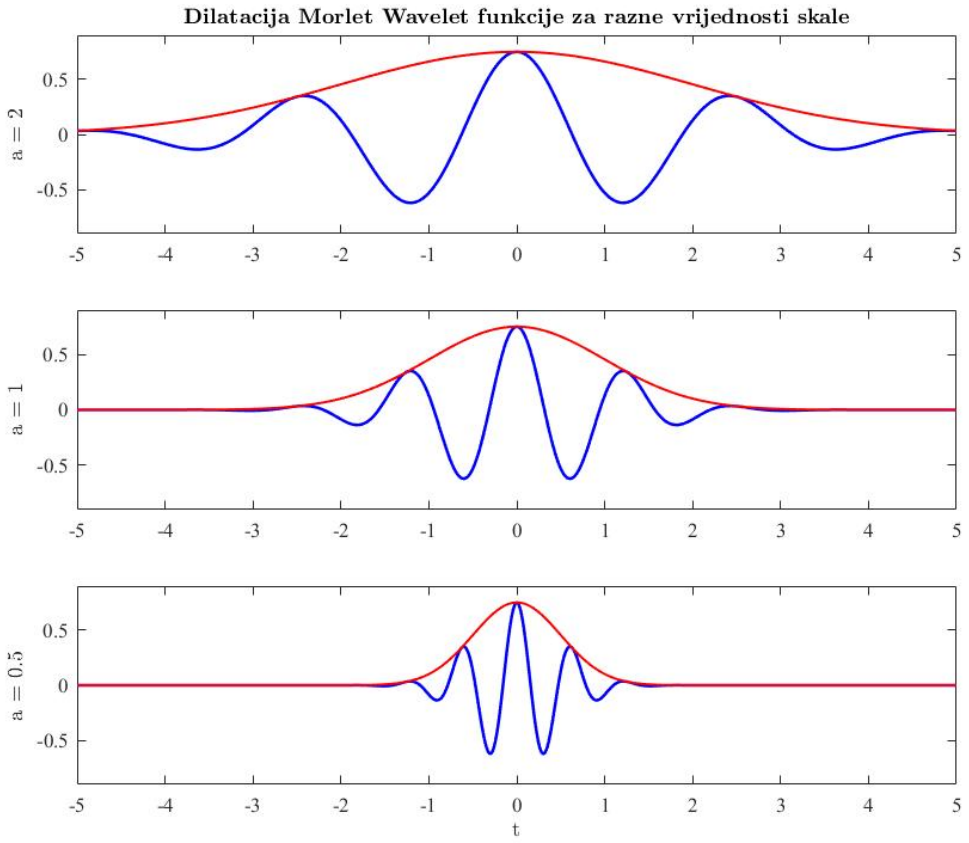
„Stepen" ovih promjena matične *Wavelet* funkcije prozora se naziva *Wavelet* skala. Za *Morlet Wavelet* funkciju prozora prikazanu na slici 1 odnos *Wavelet* skale (a) i frekvencije (Ω) je:

$$a = \frac{\Omega_0}{\Omega}, \tag{1}$$

gdje je Ω_0 centralna, osnovna, frekvencija *Morlet Wavelet* funkcije prozora, a Ω frekvencija analiziranog signala. Sa povećavanjem *Wavelet* skale, matična *Wavelet* funkcija prozora se širi u vremenskom domenu, odnosno, dobijaju se niže frekvencije u frekvencijskom domenu. Sa smanjivanjem *Wavelet* skale dobijaju više frekvencije, odnosno *Wavelet* funkcija prozora se skuplja u vremenskom domenu.

Zahvaljujući ovim osobinama *Wavelet* transformacije, moguće je zasebno analizirati komponente signala na višim i nižim frekvencijama i analizirati detalje signala koji mogu ukazati na promjene njegovih statističkih osobina, kakva je funkcija gustine vjerovatnoće signala. Ovo je čini dobrim izborom u analizi signala koji se formira na jedinicama za sinhronizovano mjerenje fazora, kao i detekciji anomalija gdje je potrebno analizirati opšti oblik signala, ali i detalje, kako bi se mogle uočiti čak i male promjene u funkciji gustine vjerovatnoće signala.

Na slici 2 je prikazan primjer dilatacije matične *Wavelet* funkcije prozora (*Morlet Wavelet*) u frekvencijskom domenu, povećavanjem nivoa *Wavelet* skale, odnosno, smanjivanjem učestanosti ove funkcije.



Slika 2: Dilatacija matične *Wavelet* funkcije na različitim nivoima skale

2.1 Lokalizacija u vremenskom i frekvencijskom domenu

Slučajni signal koji se analizira ima komponente na visokim i niskim frekvencijama, a sposobnost *Wavelet* transformacije da se prilagođava ovim frekvencijama, na osnovu skale a, doprinosi kvalitetnoj obradi signala.

Komponente signala na niskim frekvencijama sadrže informacije o opštem obliku i trendovima signala. Posmatranjem formule (1) vidi se da niska frekvencija ovih komponenti odgovara višoj *Wavelet* skali, odnosno širem *Wavelet* prozoru u vremenskom domenu i niskim frekvencijama *Wavelet* signala u frekvencijskom domenu. Visokofrekvente komponente signala sadrže informacije o detaljima signala i odgovaraju nižim *Wavelet skalama*, odnosno, užem *Wavelet* prozoru u vremenskom domenu i višim frekvencijama u frekvencijskom domenu.

2.2 Kontinualna *Wavelet* transformacija

Kontinualna *Wavelet* transformacija (eng. *Continious Wavelet transform - CWT*) je kontinualna u frekvencijskom domenu i omogućava kontinualnu promjenu skale i translaciju (u vremenskom domenu). Odnosno, matična *Wavelet* funkcija prozora podliježe kontinualnim promjenama u domenu skale i vremenskog pomjeraja, translacije. U opštem obliku kontinualna *Wavelet* transformacija se može zapisati na sljedeći način:

$$CWT(t,a) = \frac{1}{\sqrt{|a|}} \int_{-\infty}^{\infty} x(\tau)\phi^*(\frac{\tau - t}{a})d\tau, \tag{2}$$

gdje je $x(\tau)$ signal koji podliježe transformaciji, t oznaka vremenskog trenutka, τ oznaka vremenskog pomjeraja, a nivo dekompozicije i ϕ^* kompleksno konjugovana matična *Wavelet* funkcija prozora.

Viši nivoi *Wavelet* skale, a, omogućavaju analizu nižih frekvencija, dok vremenski pomjeraj τ obezbjeđuje lokalizaciju promjena u vremenskom domenu.

Kontinualna *Wavelet* transformacija se primjenjuje u slučajevima kada je precizna frekvencijska i vremenska analiza od ključnog značaja kao što je to slučaj sa seizmičkim ili bio-medicinskim signalima, [21–23]. Međutim, računanje kontinualne *Wavelet* transformacije podrazumijeva izrazitu računsku složenost, u odnosu na diskretnu *Wavelet* transformaciju (eng. *Discrete Wavelet transform - DWT*). Stoga se u praksi, posebno u rješavanju problema softverskim rješenjima, češće koristi diskretna *Wavelet* transformacija.

2.3 Diskretna *Wavelet* transformacija

Wavelet transformacija se u diskretnom obliku može predstaviti sljedećim izrazom:

$$DWT_x(j,k) = \sum_t x(t)\phi_{j,k}(t), \tag{3}$$

gdje je t vremenski trenutak, pa je $x(t)$ signal nad kojim se vrši transformacija u trenutku t, j predstavlja nivo *Wavelet* skale, k je indeks translacije u vremenu, a $\phi_{j,k}(t)$ skalirana *Wavelet* funkcija prozora u diskretnom obliku, koja se od matične *Wavelet* funkcije prozora dobija na sljedeći način:

$$\phi_{j,k}(t) = 2^{-\frac{j}{2}}\phi(2^{-j}t - k), \tag{4}$$

gdje je $\phi(t)$ matična *Wavelet* funkcija prozora u diskretnom obliku.

Prednost korišćenja diskretne *Wavelet* transformacije je, između ostalih, i manja računska složenost u odnosu na kontinualnu *Wavelet* transformaciju uz dovoljno dobru preciznost u frekvencijskom i vremenskom domenu. Ipak, u slučaju aproksimacije funkcije gustine vjerovatnoće signala se pokazuje kao bolji kandidat od kontinualne *Wavelet* transformacije zahvaljujući svom svojstvu ortogonalnosti, objašnjenom u podsekciji 2.5 i linearnoj nezavisnosti njenih funkcija.

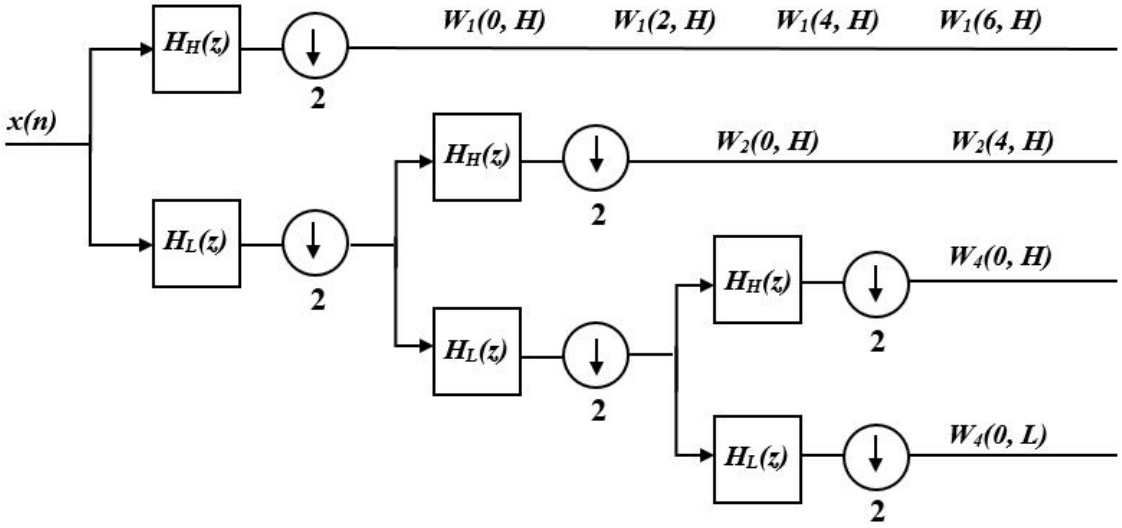
2.4 *Wavelet* transformacija kao banka filtara

Wavelet transformacija signala se može posmatrati kao sukcesivna dekompozicija signala na više i niže frekvencije po principu banke filtara. Dekompozicija se vrši prolaskom signala kroz niskopropusni filtar (eng. *low-pass filter*) i visokopropusni filtar (eng. *high-pass filter*), čime dobijamo komponente signala na niskim frekvencijama koje sadrže globalne informacije o signalu, poput oblika signala, i komponente na višim frekvencijama koje sadrže detalje signala, i koje mogu ukazivati na pojavu nekih anomalija u signalu. U svakoj iteraciji se dio signala na nižim frekvencijama ponovo dekomponuje na više i niže frekvencije, pomoću filtara odgovarajućih propusnih opsega.

Nakon dekompozicije signala na visoke i niske frekvencije, zahvaljujući *Nyquistovoj* teoremi (*Harry Nyquist*(1889.-1976.)), po kojoj signal može biti potpuno rekonstruisan ako je uzorkovan s najmanje dvostruko većom frekvencijom od najveće prisutne frekvencije u signalu, [24], nad dobijenim komponentama niske frekvencije se vrši smanjivanje uzorka (eng. *downsampling*) faktorom 2. Odnosno, dalje će se analizirati svaka druga komponenta signala, u frekvencijskom domenu, dobijena nakon filtriranja.

Propuštanje signala kroz filtar niskog propusnog opsega eliminišu se komponente iznad polovine nove frekvencije uzorkovanja i time se sprječava preklapanje frekvencijskih komponenti (eng. *aliasing*). Na taj način izbjegava se gubitak informacija i distorzija prilikom rekonstrukcije signala, dok se omogućavanjem redukcije uzoraka faktorom 2 smanjuje količina redundantnih podataka u signalu.

Primjer jedne dekompozicije signala *Wavelet* transformacijom je dat na slici 3, gdje *Wavelet* skala ima 3 nivoa.



Slika 3: Dekompozicija signala *Wavelet* transformacijom kao bankom filtara

Na prvom nivou, nakon filtriranja ostaju komponente na visokim frekvencijama, dok se na drugom i trećem nivou obrađuju komponente nižih frekvencija. Na svakom nivou dekompozicije se obavlja i redukcija uzoraka (eng. *downsampling*), odnosno, uzima se svaka druga komponenta kako bi se otklonili redudantni podaci. S obzirom na to da se radi o nižim frekvencijama, moguće je ukloniti dio signala bez gubitka informacija.

2.5 Osobina ortogonalnosti

U cilju kvalitetne rekonstrukcije signala, važan uslov koji banka filtara mora ispunjavati je da impulsni odzivi filtara moraju biti ortogonalni u odnosu na svoje prethodnike, odnosno, u odnosu na impulsne odzive filtara na višim frekvencijama. Moraju biti ortogonalni sa pomakom od dvije komponente ili više, u zavisnosti od toga kojim brojem je redukovan filtrirani uzorak, kako bi se obezbijedila međusobna nezavisnost komponenata signala i smanjila redudantnost. Ortogonalnost omogućava proces suprotan smanjenju broja uzoraka, jer se signal može rekonstruisati dodavanjem nula između uzoraka, na pozicije uklonjenih uzoraka, i filtriranjem (eng. *upsampling*), čime se ostvaruje reverzibilnost transformacije, odnosno potpuna i precizna rekonstrukcija originalnog signala bez gubitka informacije.

Ortogonalnost impulsnih odziva filtara se izražava sljedećim izrazom:

$$\langle h_L(m), h_L(m-2n)\rangle = \delta(n), \tag{5}$$

$$\sum_m h_L(m)h_L(m-2n) = \delta(n), \tag{6}$$

gdje je h_L impulsni odziv filtra, dok su m i n vremenske oznake, $\delta(n)$ Dirakov impuls, a $\langle\rangle$ predstavlja operaciju unutrašnjeg proizvoda [20].

Impulsni odziv je ortogonalan u odnosu na svoju frekvencijski pomjerenu komponentu u frekvencijskom domenu ukoliko zadovoljava uslov:

$$|H_L(e^{j\omega})|^2 + |H_L(e^{j(\omega+\pi)})|^2 = 2, \tag{7}$$

U praksi, ovo označava da za uspješnu i kvalitetnu rekonstrukciju signala, matična i skalirana *Wavelet* funkcija prozora moraju biti međusobno ortogonalne [20]. Odnosno, da formiraju ortogonalni vektorski prostor, tako da su ove funkcije uvijek međusobno ortogonalne, bez obzira na broj modifikacija i transliranja skalirane *Wavelet* funkcije, i da kao takve predstavljaju ortogonalne vektorske baze.

Kontinualna *Wavelet* transformacija nije ortogonalna vektorska baza koja zadovoljava uslov za aproksimaciju funkcije gustine vjerovatnoće signala. *Wavelet* funkcije koje su kontinualne nisu međusobno linearno nezavisne i prilikom njihovog korišćenja u svrhu aproksimacije funkcije gustine vjerovatnoće signala došlo bi do pojavljivanja redudantnih skaliranih i diletiranih vrijednosti signala što bi negativno uticalo na aproksimaciju [20].

Nasuprot kontinualnoj *Wavelet* transformaciji, diskretna *Wavelet* transformacija je diskretizovana u vremenskom i frekvencijskom domenu i kao takva može činiti ortogonalnu vektorsku bazu [25]. Takođe, njena diskretizacija u oba domena uprošćava računsku složenost koju bi imala kontinualna *Wavelet* transformacija i zbog toga je bolji kandidat u aproksimaciji funkcije gustine vjerovatnoće signala od kontinualne *Wavelet* transformacije. Stoga, diskretna *Wavelet* transformacija može biti dio rješenja problema u različitim oblastima, zavisno od izbora vrste (porodice) *Wavelet* funkcije prozora.

2.6 *Wavelet* porodice

Wavelet funkcije prozora pripadaju različitim porodicama od kojih svaka ima specifične osobine i prednosti. *Wavelet* porodice međusobno se razlikuju prema obliku, vremensko-frekvencijskoj lokalizaciji, ortogonalnosti, simetriji i glatkoći, što omogućava njihovu upotrebu u specifičnim problemima analize signala.

Po ortogonalnosti, *Wavelet* porodice se dijele na one sa ortogonalnim, neortogonalnim i biortogonalnim funkcijama. U zavisnosti od primjene, mogu biti efikasan alat u rješavanju izuzetno kompleksnih problema.

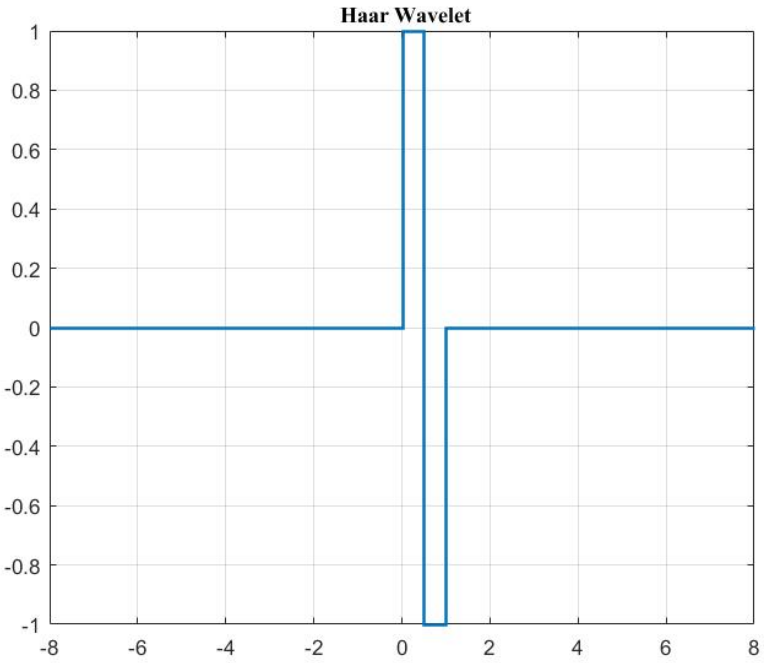
Primjeri porodica koje formiraju ortogonalne vektorske baze su *Haar, Daubechies, Symlet* i *Coiflet*. Funkcije prozora ovih porodica su pogodne za rješavanje problema aproksimacije funkcije gustine vjerovatnoće signala i detekciju GPS *spoofing* napada.

2.6.1 Haar Wavevelet

Haar Wavelet predstavlja najjednostavniji oblik *Wavelet* funkcije prozora, uveden 1910. godine od strane mađarskog naučnika *Alfred*-a *Haar*-a(1885.-1993.). Osnovna funkcija prozora ove porodice ima oblik pravougaonih impulsa i efikasna je u detekciji ivica slike ili naglih promjena signala, [26]. Njen oblik se može predstaviti sljedećim izrazom:

$$\phi(t) = \begin{cases} 1, & 0 \leq t < \frac{1}{2}, \\ -1, & \frac{1}{2} \leq t < 1, \\ 0, & \text{inače.} \end{cases} \tag{8}$$

Prednost *Haar Wavelet* transformacije je u njenoj izuzetnoj jednostavnosti koja omogućava laku implementaciju. Na slici 4 je predstavljena njena matična *Wavelet* funkcija prozora.

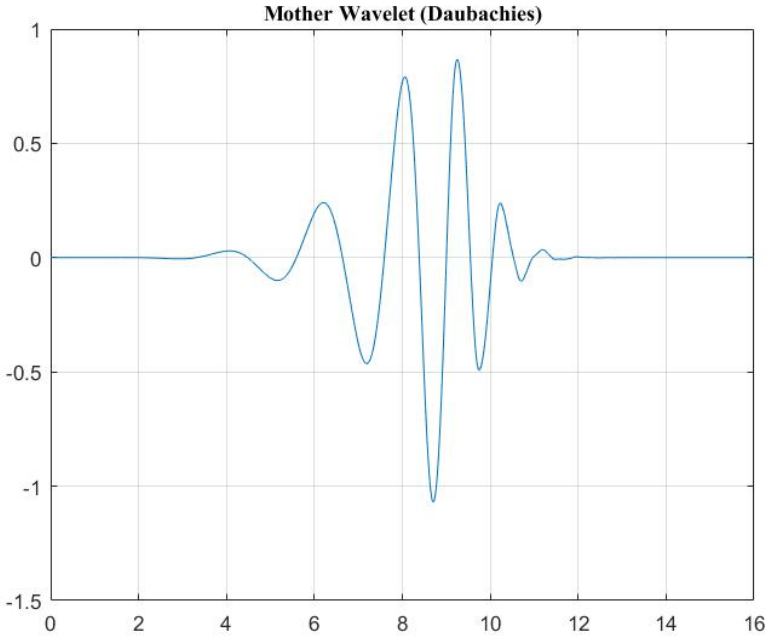


Slika 4: Osnovni oblik *Haar Wavelet* transformacije

Oštri prelaz između dvije vrijednosti, 1 i -1, je efikasan alat pri detekciji naglih promjena analiziranog signala, što ovu porodicu čini prikladnim kandidatom u slučaju estimacije funkcije gustine vjerovatnoće signala i detekcije njene promjene.

2.6.2 *Daubechies Wavelet*

Još jedna *Wavelet* porodica čije funkcije prozora zadovoljavaju uslov ortogonalnosti je *Daubechies Wavelet*, prikazan na slici 5. Naučnom svijetu ga je 1988. godine predstavila belgijska matematičarka *Ingrid Daubechies*(1954-danas). Za razliku od *Haar Wavelet* transformacije, oblik ove funkcije prozora je glatkiji, što se može primijetiti i golim okom, i to obezbjeđuje bolju rekonstrukciju originalnog signala. Kao i *Haar Wavelet* funkcija prozora, ima kompaktnog nosioca, odnosno, ograničena je na malom vremenskom intervalu, [27].

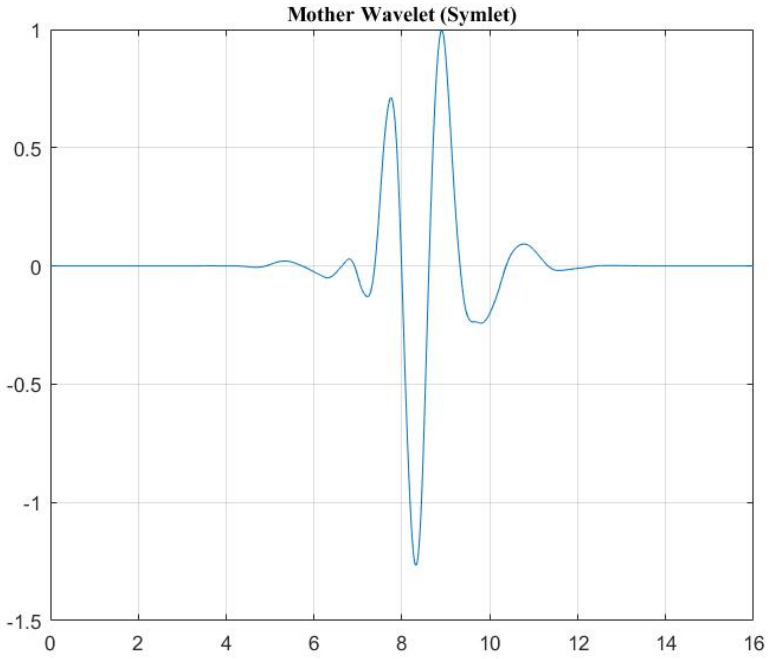


Slika 5: *Daubechies Wavelet* u osnovnom obliku, reda 9

Na slici 5 je predstavljena matična *Wavelet* funkcija prozora *Daubechies Wavelet* porodice, reda 9. Red *Wavelet* funkcije prozora označava red polinoma koji *Wavelet* funkcija prozora može aproksimirati. Funkcije prozora *Daubechies Wavelet* porodice mogu tačno aproksimirati polinome do 9. reda.

2.6.3 Symlet Wavelet

Za razliku od *Daubechies Wavelet* porodice, *Symlet Wavelet* porodica sadrži funkcije prozora koje su skoro simetrične, odnosno skoro parne $\psi(t) \approx \psi(-t)$. Predložene od strane *Ingrid Daubechies*, *Symlet Wavelet* funkcije prozora predstavljaju poboljšanu verziju *Daubechies Wavelet* funkcija prozora u pogledu simetrije. Osim simetrije, zadržavaju sve ostale osobine *Daubechies Wavelet* porodice. Kao i funkcije prozora *Daubechies Wavelet* porodice, mogu aproksimirati veliki broj različitih kompleksnih funkcija, a time i funkciju gustine vjerovatnoće slučajnog signala. U odnosu na funkcije prozora *Daubechies Wavelet* porodice, zbog svoje simetričnosti u odnosu na središnju tačku talasnog oblika, *Symlet Wavelet* funkcije prozora su efikasniji alat u rješavanju problema uklanjanja šuma sa signala i procesima obrade slike, [28].

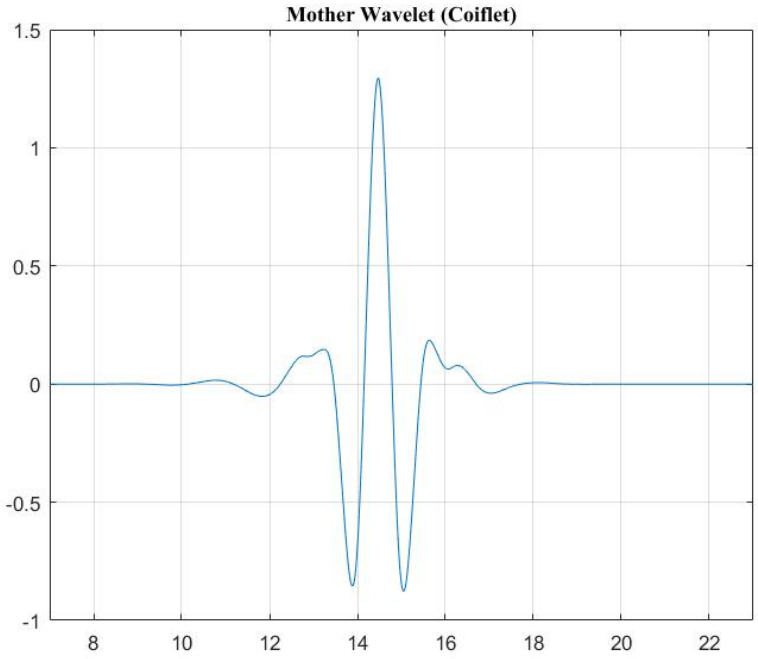


Slika 6: Osnovni oblik *Symlet Wavelet* funkxije, reda 9

Na slici 6 je prikazan osnovni oblik funkcije prozora *Symlet Wavelet* porodice, reda 9. Ove funkcije prozora, kao i funkcije prozora *Daubechies Wavelet* porodice, mogu aproksimirati polinome do 9. stepena.

2.6.4 *Coiflet Wavelet*

Četvrta grupa ortogonalnih *Wavelet* funkcija prozora je *Coiflet Wavelet*. Dolazi kao rezultat dugogodišnjih istraživanja *Ingrid Daubechies* i predstavlja još jednu verziju *Daubechies Wavelet* funkcija prozora, međutim, sa većim brojem nultih momenata (eng. *vanishing moments*). U funkcijama prozora *Coiflet Wavelet* porodice nulti momenti se pojavljuju i u slučaju skalirane *Wavelet* funkcije prozora, a omogućavaju efikasno uklanjanje niskofrekventnih komponenti signala. Time poboljšavaju detekciju anomalija signala. Upravo zbog ove osobine su još jedno adekvatno rješenje u slučaju aproksimacije funkcije gustine vjerovatnoće signala i detekcije promjena u njenoj strukturi, [28].



Slika 7: Osnovni oblik *Coiflet Wavelet*-a, reda 5

Na slici 7 je prikazan osnovni oblik, matična *Wavelet* funkcija prozora *Coiflet Wavelet* porodice. Poboljšanje simetrije njenog oblika, u odnosu na središnju tačku talasnog oblika, u poređenju sa prethodno opisanim porodicama je vidljiva i golim okom. Kao i u slučaju *Symlet Wavelet* funkcija prozora, ovo je čini pogodnom u slučajevima uklanjanja šuma na slikama i u signalima, kao i u slučaju aproksimacije velikog broja različitih funkcija.

Prednost korišćenja *Wavelet* transformacije u cilju aproksimacije funkcije gustine vjerovatnoće signala je u tome što *Wavelet* funkcije imaju mogućnost postizanja dobre globalne aproksimacije signala zahvaljujući mogućnosti obrade detalja signala analizom na različitim nivoima *Wavelet* skale, [25]. Ovo takođe izaziva osjetljivost *Wavelet* transformacije na brze i nagle promjene signala i čini je pogodnom osnovom za detekciju promjene funkcije gustine vjerovatnoće signala.

2.7 Estimacija funkcije gustine vjerovatnoće signala korišćenjem *Wavelet* transformacije

Estimacija neke funkcije se može izvršiti linearnom kombinacijom funkcija koje predstavljaju ortogonalne vektorske baze i nazivaju se bazne funkcije, što je prvi put predstavljeno u radu [29].

Na osnovu zapažanja iz prethodnog poglavlja se može zaključiti da se nepoznata funkcija gustine vjerovatnoće signala x može estimirati korišćenjem *Wavelet* ortogonalnih baza i diskretne *Wavelet* transformacije, i to se može učiniti na osnovu sljedećeg izraza:

$$p(x) = \sum_{j_0,k} \alpha_{j_0,k}\phi_{j_0,k}(x) + \sum_{j \geq j_0,k}^{\infty} \beta_{j,k}\psi_{j.k}(x), \tag{9}$$

gdje su $\phi(x)$ i $\psi(x)$ matična i skalirana *Wavelet* funkcija prozora, respektivno, j_0 osnovni, nulti, nivo *Wavelet* skale na kom se nalazi matična *Wavelet* funkcija prozora, k broj pomjeraja skalirane *Wavelet* funkcije prozora u vremenskom domenu, a j trenutni nivo *Wavelet* skale skalirane *Wavelet* funkcije prozora. Koeficijenti α i β određuju uticaj matične i skalirane *Wavelet* funkcije prozora na aproksimaciju funkcije gustine vjerovatnoće signala i igraju ključnu ulogu u kvalitetu aproksimacije. Ovi koeficijenti predstavljaju srednju vrijednost odbiraka matične i skalirane *Wavelet* funkcije prozora, respektivno, [30].

Ako je signal $x(t)$ nezavisan i identično distribuiran (eng. *independent and identically distributed - iid*) signal sa N odbiraka, *Wavelet* koeficijente α i β možemo predstaviti sljedećim izrazima:

$$\alpha_{j_0,k} = \frac{1}{N}\sum_{n=1}^{N} \phi_{j_0,k}(x_n) \quad \beta_{j,k} = \frac{1}{N}\sum_{n=1}^{N} \psi_{j,k}(x_n) \tag{10}$$

Posmatranjem prethodno navedenog izraza se uočava još jedan problem koji bi nastao korišćenjem kontinualne *Wavelet* transformacije u ovom procesu. Naime, konvolucijom dva kontinualna signala nastao bi beskonačan broj koeficijenata, [20], što je i razlog više za korišćenje diskretne *Wavelet* transformacije u procesu aproksimacije funkcije gustine vjerovatnoće signala i detekcije njenih promjena.

3 Detekcija promjene funkcije gustine vjerovatnoće signala

Detekcija promjene funkcije gustine vjerovatnoće signala predstavlja jednu od važnih tehnika analize nepoznatog slučajnog signala i njegovih karakteristika. Metode detekcije se najčešće realizuju u dva koraka, estimacijom funkcije gustine vjerovatnoće signala, a zatim računanjem razlike između parametara estimacije distribucije na različitim djelovima signala. Računanje razlike se može obavljati metodom najmanjih kvadrata (eng. *LSM - Least Square Method*) [7], entropijom [3], mjerom maksimalne vjerovatnoće [31], a sama estimacija funkcije gustine vjerovatnoće signala može se obavljati metodama sa **parametarskim** i **neparametarskim** pristupom.

Metode sa parametarskim pristupom pretpostavljaju da funkcija gustine vjerovatnoće može biti opisana modelom sa ograničenim brojem parametara, koji se zatim estimiraju iz podataka. Tipičan primjer ovakvog pristupa je mjera maksimalne vjerovatnoće.

Metode sa neparametarskim pristupom ne polaze od pretpostavke da funkcija gustine vjerovatnoće ima unaprijed poznat matematički oblik. Umjesto toga, one omogućavaju fleksibilno određivanje te funkcije direktno iz podataka, uz određene uslove, kao što je glatkoća (eng. *smoothness*) ili pripadnost funkcije nekoj ograničenoj, ali beskonačno-dimenzionalnoj klasi, kao što su ortogonalne vektorske baze. Na taj način se funkcija prilagođava strukturi podataka, bez ograničavanja na fiksni broj parametara.

3.1 Histogram

Histogram je standardna neparametarska metoda koja se tradicionalno koristi kao statistička metoda za vizuelnu inspekciju anomalija u vrijednostima signala i analizu njegove distribucije, kao u [32].

Neka su $x_1, ..., x_n$ uzorci signala, koji slijede funkciju gustine vjerovatnoće $f(x)$ sa osobinom:

$$\int f(x)dx = 1 \quad \text{ako je} \quad f(x) \geq 0 \quad \text{za svako } x,$$

i neka je histogram funkcije $f(x)$ obilježen kao $\hat{f}_H(x)$.

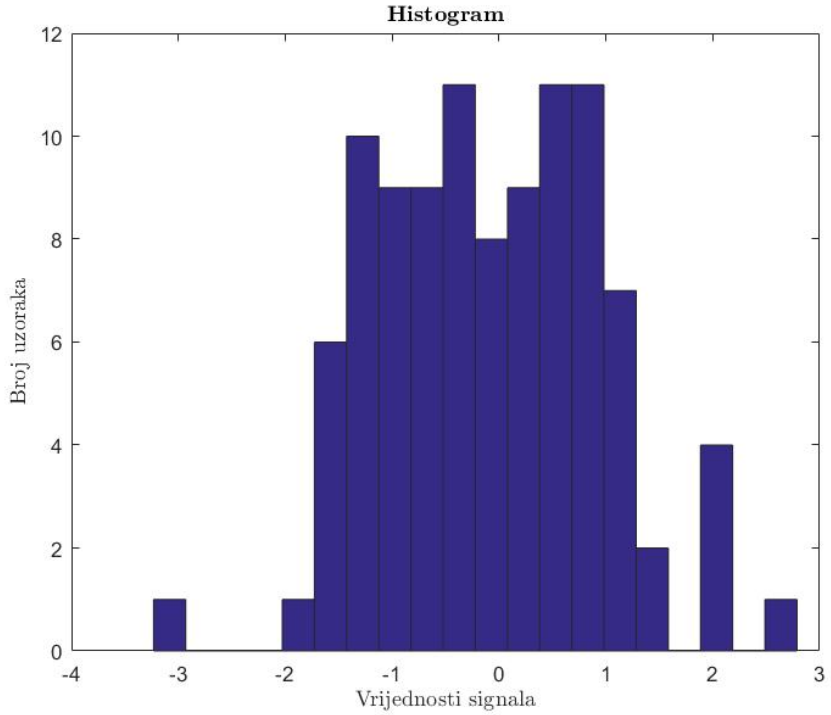
Uzorci signala $x_1, ..., x_n$ se dijele na $m = m(n)$ podskupova, koji će na histogramu biti predstavljeni stupcima, B_j, $j = 1, ..., m$. Neka je m_j broj uzoraka signala koji pripada podskupu B_j, a $|B_j|$ širina tog podskupa. Ukoliko odbirak x pripada podskupu B_l, a m_l je broj uzoraka koji pripada tom podskupu, onda je aproksimacija

funkcije gustine vjerovatnoće signala histogramom data izrazom, [32]:

$$\hat{f}_H(x) = \frac{m_l}{\sum_{j=1}^{m} m_j |B_j|}. \tag{11}$$

Iako ovaj metod daje jednostavno rješenje estimacije funkcije gustine vjerovatnoće signala, njegov rezultat je predstavljen diskretnim vrijednostima, stupcima što uvodi diskontinuitet u ovoj aproksimaciji i ne čini ga optimalnim rješenjem.

Na slici 8 je prikazan histogram slučajnog signala, koji je podijeljen u 20 podskupova (binova), odnosno za koji važi $m = 20$.



Slika 8: Estimacija funkcije gustine vjerovatnoće signala histogramom

3.2 Detekcija promjene funkcije gustine vjerovatnoće signala metodom procjene maksimalne vjerovatnoće

Detekcija promjene funkcije gustine vjerovatnoće mjerom maksimalne vjerovatnoće se najčešće obavlja korišćenjem dva prozora i podrazumijeva dva koraka:

1. Estimaciju funkcije gustine vjerovatnoće djelova signala obuhvaćenog prozorima;

2. Računanje mjere maksimalne vjerovatnoće između ovih distribucija.

Funkcija gustine vjerovatnoće se može estimirati histogramom, kako je opisano u podsekciji 3.1, ili pretpostavljanjem normalne (Gausove) funkcije raspodjele u posmatranom signalu i estimiranjem parametara ove distribucije, srednje vrijednosti μ i standardne devijacije σ, nakon čega se vrši računanje mjere maksimalne vjerovatnoće između parametara estimacije.

Bilo da su funkcije gustine vjerovatnoće estimirane histogramom ili se estimiraju parametri pretpostavljene normalne funkcije gustine vjerovatnoće, računanje razlike između parametara estimiranih funkcija gustine vjerovatnoće se obavlja računanjem sume logaritamskih odnosa između distribucija:

$$d_{MLE} = |\sum_{t} \log_2(\frac{f_{novo}(t+T)}{f_{referentno}(t)})| \tag{12}$$

gdje je $f_{novo}(t+T)$ vrijednost estimirane funkcije gustine vjerovatnoće signala u prozoru koji obuhvata nadolazeći signal u trenutku (t+T), T je širina referentnog prozora, a $f_{referentno}(t)$ vrijednost estimirane funkcije gustine vjerovatnoće signala u referentnom prozoru u trenutku t, tj. prozoru koji obuhvata dio signala na kom se smatra da nema promjene funkcije gustine vjerovatnoće signala.

S obzirom na to da detekcija promjene funkcije gustine vjerovatnoće signala mjerom maksimalne vjerovatnoće podrazumijeva proces od dva koraka, odnosno, estimaciju funkcije gustine vjerovatnoće signala estimacijom parametara pretpostavljene funkcije gustine vjerovatnoće signala i računanje razlike između estimiranih vrijednosti, ovo može biti vremenski i memorijski izazovan proces što ga ne čini pogodnim za rad sa velikim količinima podataka, kao ni za rad u realnom vremenu.

3.3 Detekcija promjene funkcije gustine vjerovatnoće signala zasnovana na entropiji

Slično procesu detekcije promjene funkcije gustine vjerovatnoće signala mjerom maksimalne vjerovatnoće, detekcija zasnovana na entropiji se može obaviti računanjem entropije između estimiranih distribucija signala. Kao i prethodno opisan metod, proces se obavlja korišćenjem dva prozora u dva koraka:

1. Estimacijom funkcije gustine vjerovatnoće signala korišćenjem histograma ili pretpostavljanjem normalne distribucije signala i estimacijom parametara normalne distribucije;
2. Računanjem **relativne entropije**, ili *Kullback-Leibler* divergencije, između ovih distribucija [2].

Relativna entropija između ovih distribucija se može definisati kao mjera udaljenosti ditribucije računate na nadolazećem signalu od distribucije signala računate u referentnom prozoru, odnosno, prozoru za koji se smatra da obuhvata originalni signal, bez promjene. Može se predstaviti sljedećim izrazom:

$$d_E = \sum_t |p_{novo}(t+T) - p_{referentno}(t)| \log_2(|p_{novo}(t+T) - p_{referentno}(t)|) \qquad (13)$$

gdje je $p_{novo}(t+T)$ vrijednost estimirane funkcije gustine vjerovatnoće signala u prozoru koji obuhvata nadolazeći signal u trenutku $t+T$, T je širina referentnog prozora, dok je $p_{referentno}(t)$ vrijednost funkcije gustine vjerovatnoće signala računate u referentnom prozoru u trenutku t, odnosno, u prozoru koji obuhvata dio signala na kom se pretpostavlja da nema promjene funkcije gustine vjerovatnoće signala.

Isto kao i detekcija promjene funkcije gustine vjerovatnoće signala mjerom maksimalne vjerovatnoće, metod detekcije promjene distribucije signala računanjem relativne entropije podrazumijeva postupak od dva koraka, od kojih je prvi estimacija funkcije gustine vjerovatnoće i samim tim može biti vremenski i memorijski zahtjevan proces prilikom rada sa velikom količinom podataka ili detekcije promjena u realnom vremenu.

3.4 Detekcija promjene funkcije gustine vjerovatnoće signala posredstvom *Wavelet* transformacije

Metod detekcije promjene funkcije gustine vjerovatnoće signala koja se zasniva na *Wavelet* transformaciji koristi *Wavelet* funkcije prozora kao bazne funkcije u procesu estimaciju funkcije gustine vjerovatnoće [7].

Estimacija funkcije gustine vjerovatnoće se, na osnovu [29], može predstaviti slično kao u formuli 9, s tim što se koristi diskretna *Wavelet* transformacija kao bazna funkcija sa konačnim brojem translacija i dilatacija signala. Estimacija može biti predstavljena sljedećim izrazom:

$$p(x) = \sum_{l=1}^{L} \hat{\alpha}_{j_0,l}\phi_{j_0,l}(x) + \sum_{j=j_0}^{J}\sum_{l=1}^{L_j} \hat{\beta}_{j,l}\psi_{j,l}(x) \tag{14}$$

gdje su $\phi_{j_0,l}(x) = 2^{\frac{j_0}{2}}\psi(2^{j_0}x - l)$ matična *Wavelet* funkcija prozora, $\psi_{j,l}(x) = 2^{\frac{j}{2}}\psi(2^j x - l)$ skalirana *Wavelet* funkcija prozora, j_0 početni nivo *Wavelet* skale na kom se nalazi matična *Wavelet* funkcija prozora, j trenutni nivo *Wavelet* skale skalirane *Wavelet* funkcije prozora, l indeks trenutne translacije funkcije, L maksimalan broj translacija matične *Wavelet* funkcije, L_j maksimalan broj translacija skalirane *Wavalet* funkcije prozora na trenutnom nivou *Wavelet* skale j [7].

Koeficijenti $\hat{\alpha}$ i $\hat{\beta}$ igraju veoma važnu ulogu u samoj preciznosti estimacije funkcije gustine vjerovatnoće signala. Sljedeći izrazi predstavljaju vrijednost $\hat{\alpha}$ koeficijenta na nultom nivou, j_0, *Wavelet* skale, u toku l-te translacije, i vrijednost $\hat{\beta}$ koeficijenta na j-tom nivou *Wavelet* skale, u toku l-te translacije:

$$\hat{\alpha}_{j_0,l} = \frac{1}{N}\sum_{n=1}^{N}\psi_{j_0,l}(x_n) \quad \text{i} \quad \hat{\beta}_{j,l} = \frac{1}{N}\sum_{n=1}^{N}\psi_{j,l}(x_n), \tag{15}$$

gdje matična i skalirana *Wavelet* funkcija prozora moraju pripadati *Wavelet* porodici koja ima ortogonalne baze.

Detekcija promjene funkcije gustine vjerovatnoće signala podrazumijeva korišćenje dva prozora u kojima se posmatra signal. Jedan prozor je referentni, odnosno, obuhvata dio signala gdje se pretpostavlja nepromjenljiva funkcija gustine vjerovatnoće signala. Drugi prozor obuhvata nadolazeći signal, odnosno njime se analizira dio signala na kom se pretpostavlja pojava promjene funkcije gustine vjerovatnoće signala. U najvećem broju metoda, među kojima su i prethodno opisane metode detekcije računanjem relativne entropije i mjerom maksimalne vjerovatnoće, prvo se vrši estimacija funkcije gustine vjerovatnoće intervala signala obuhvaćenih vremenskim prozorima i nakon toga se računa razlika između estimacija. Trenutak promjene

funkcije gustine vjerovatnoće signala se proglašava onda kada vrijednost ove razlike bude veća od neke predifinasne vrijednosti praga.

Za razliku od metoda zasnovanih na entropiji i mjeri maksimalne vjerovatnoće, prednost ovog metoda je i to da nije potrebno eksplicitno računati estimaciju funkcije gustine vjerovatnoće signala.

3.4.1 Direktno računanje $L2$ mjere između funkcija gustine vjerovatnoće signala korišćenjem *Wavelet* koeficijenata

Detekcija promjene funkcije gustine vjerovatnoće signala se vrši računanjem $L2$ mjere između funkcija gustine vjerovatnoće signala estimiranih u toku dva odvojena vremenska intervala. Analitička razlika između ovih distribucija, $f(x) = p_1(x) - p_2(x)$, gdje su $p_1(x)$ i $p_2(x)$ distribucije signala u intervalima dužine N sa odbircima $\{x_{1n}\}_{n=1}^{N}$ i $\{x_{2n}\}_{n=1}^{N}$, respektivno, se može izračunati minimizacijom kvadratne greške između analitičke razlike, $f(x)$ i njene estimirane vrijednosti $g(x)$ na sljedeći način:

$$\arg\min_{g} \int (g(x) - f(x))^2 dx, \tag{16}$$

gdje je estimirana razlika između funkcija gustine vjerovatnoće signala u dva odvojena vremenska intervala predstavljena kao u (14):

$$g(x) = \sum_{l} \alpha_{j_0,l}\phi_{j_0,l}(x) + \sum_{j=j_0}^{J}\sum_{l} \beta_{j,l}\psi_{j,l}(x), \tag{17}$$

ili u matričnoj formi kao:

$$g(x) = \boldsymbol{\Phi}^T(x)\boldsymbol{\alpha} + \sum_{j=j_0}^{J} \boldsymbol{\Psi}^T(x)\boldsymbol{\beta}_j, \tag{18}$$

gdje je $\boldsymbol{\Phi(x)}$ matrica matične *Wavelet* funkcije, na nivou *Wavelet* skale j_0 i $\boldsymbol{\Psi(x)}$ matrica skalirane *Wavelet* funkcije, na nivou *Wavelet* skale j. $\boldsymbol{\alpha} \in \mathbb{R}^{L\times 1}$ je vektor *Wavelet* koeficijenata na j_0 nivou *Wavelet* skale, a $\boldsymbol{\beta} \in \mathbb{R}^{L_j\times 1}$ je vektor *Wavelet* koeficijenata na j nivou *Wavelet* skale i njihove vrijednosti su:

$$\boldsymbol{\alpha} = [\alpha_{j_0,1}, ..., \alpha_{j_0,L}]^T \quad \text{i} \quad \boldsymbol{\beta} = [\beta_{j,1}, ..., \beta_{j,L_j}]^T \tag{19}$$

Izraz (16) se može razviti preko kvadrata razlike u:

$$\arg\min_{g} = \int (g^2(x) - 2g(x)f(x) + f^2(x))dx, \tag{20}$$

S obzirom na to da je cilj dobiti aproksimaciju razlike distribucija $g(x)$ moguće je zanemariti član $f^2(x)$, [33], te se izraz (20) može zapisati na sljedeći način:

$$\arg\min_{g} = \int (g^2(x) - 2g(x)f(x))dx, \tag{21}$$

Matična i skalirana *Wavelet* funkcija prozora su ortogonalne vektorske baze, i stoga važi $\boldsymbol{\Phi}\boldsymbol{\Phi}^T = \boldsymbol{I} \in \mathbb{R}^{L\times L}$, $\boldsymbol{\Psi}_j\boldsymbol{\Psi}_j^T = \boldsymbol{I} \in \mathbb{R}^{L_j\times L_j}$, $\boldsymbol{\Psi}_j\boldsymbol{\Psi}_k^T = \mathbf{0} \in \mathbb{R}^{L_j\times L_k}$ za $j \neq k$ i da je $\boldsymbol{\Phi}\boldsymbol{\Psi}_j^T = \mathbf{0} \in \mathbb{R}^{L\times L_j}$, a izraz (21) se može svesti na:

$$\begin{aligned}\arg\min_{\alpha,\beta_j} \Bigg\{ &\boldsymbol{\alpha}^T\boldsymbol{\alpha} - 2\boldsymbol{\alpha}^T \int \boldsymbol{\Phi}(x)(p_1(x) - p_2(x))dx \quad + \\ &\sum_{j=j_0}^{J} \left(\boldsymbol{\beta}_j^T\boldsymbol{\beta}_j - 2\boldsymbol{\beta}_j^T \int \boldsymbol{\Psi}_j(x)(p_1(x) - p_2(x))dx \right),\end{aligned} \tag{22}$$

Sada se (22) može posmatrati kao optimizacioni algoritam po dvije promjenljive, α i β, odnosno po *Wavelet* koeficijentima, i izraz se može zapisati u obliku dvije odvojene komponente:

$$\boldsymbol{\alpha}^* = \arg\min_{\alpha} \left\{ \boldsymbol{\alpha}^T\boldsymbol{\alpha} - 2\boldsymbol{\alpha}^T \left(\int \boldsymbol{\Phi}(x)p_1(x)dx - \int \boldsymbol{\Phi}(x)p_2(x)dx \right) \right\}, \tag{23}$$

$$\boldsymbol{\beta}_j^* = \arg\min_{\boldsymbol{\beta}_j} \left\{ \boldsymbol{\beta}_j^T\boldsymbol{\beta}_j - 2\boldsymbol{\beta}_j^T \left(\int \boldsymbol{\Psi}_j(x)p_1(x)dx - \int \boldsymbol{\Psi}_j(x)p_2(x)dx \right) \right\}, \tag{24}$$

Integrali u izrazima (23) i (24) predstavljaju matematička očekivanja matične i skalirane *Wavelet* funkcije prozora, te se ovi izrazi mogu definisati po matičnoj i skaliranoj *Wavelet* funkciji prozora kao:

$$\mathbf{h}_{\Phi}(x) = \mathbf{E}\{\boldsymbol{\Phi}(x)\}_{p_1(x)} - \mathbf{E}\{\boldsymbol{\Phi}(x)\}_{p_2(x)}, \tag{25}$$

$$\mathbf{h}_{\Psi_j}(x) = \mathbf{E}\{\boldsymbol{\Psi}_j(x)\}_{p_1(x)} - \mathbf{E}\{\boldsymbol{\Psi}_j(x)\}_{p_2(x)}, \tag{26}$$

gdje je $\mathbf{E}\{\cdot\}$ operator matematičkog očekivanja. Za posmatrani konačni i diskretni skup vrijednosti, $\{x_n\}_{n=1}^N, x \in \mathbb{R}$, na kom se računa distribucija signala $p(x)$. Matematička očekivanja matične i skalirane *Wavelet* funkcije prozora postaju $\boldsymbol{\Phi} \in \mathbb{R}^{L\times N}$ i $\boldsymbol{\Psi}_j \in \mathbb{R}^{L_j\times N}$, gdje su $\boldsymbol{\Phi}$ i $\boldsymbol{\Psi}$ vektori matične *Wavelet* funkcije prozora na j_0 nivou *Wavelet* skale i skalirane *Wavelet* funkcije prozora na j nivou *Wavelet* skale, respektivno. Vektori su definisani na sljedeći način:

$$\boldsymbol{\Phi} = [\phi_{j_0}(x_1), ..., \phi_{j_0}(x_N)] \quad \text{i} \quad \boldsymbol{\Psi_j} = [\psi_j(x_1), ..., \psi_j(x_N)], \tag{27}$$

gdje je $\phi_{j_0}(x_n) = [\phi_{j_0,1}(x_n), ..., \phi_{j_0,L}(x_n)]^T \in \mathbb{R}^{L\times 1}$ matična *Wavelet* funkcija prozora na j_0 nivou *Wavelet* skale u n-tom vremenskom trenutku, a $\psi_j(x_n)$ skalirana *Wavelet*

funkcija prozora na j nivou *Wavelet* skale u n-tom vremenskom trenutku definisana kao: $\psi_j(x_n) = [\phi_{j,1}(x_n), ..., \psi_{j,L_j}(x_n)]^T \in \mathbb{R}^{L_j \times 1}$, ortogonalne baze definisane za različite odbirke signala $x_n (n = 1, ..., N)$.

Uzimajući u obzir vrijednosti iz (27) i činjenicu da je vjerovatnoća pojavljivanja svake od ovih vrijednosti, $p(x_n)$, ista, izrazi (25) i (26) postaju:

$$\hat{\mathbf{h}}_{\Phi} \approx \frac{1}{N}\sum_{n=1}^{N}\phi_{j_0}(x_{1n}) - \frac{1}{N}\sum_{n=1}^{N}\phi_{j_0}(x_{2n}), \tag{28}$$

$$\hat{\mathbf{h}}_{\Psi_j} \approx \frac{1}{N}\sum_{n=1}^{N}\psi_{j}(x_{1n}) - \frac{1}{N}\sum_{n=1}^{N}\psi_{j}(x_{2n}), \tag{29}$$

gdje je važno istaći da su $\hat{\mathbf{h}}_{\Phi}$ i $\hat{\mathbf{h}}_{\Psi_j}$ vektori definisani kao $\hat{\mathbf{h}}_{\Phi} = [\hat{h}_{\phi_{j_0,1}}, ..., \hat{h}_{\phi_{j_0,L}}] \in \mathbb{R}^{L\times 1}$ i $\hat{\mathbf{h}}_{\Psi_j} = [\hat{h}_{\psi_{j,1}}, ..., \hat{h}_{\psi_{j,L_j}}] \in \mathbb{R}^{L_j\times 1}$. Elementi u trenutku l-te translacije ovih vektora su definisani na sljedeći način:

$$\hat{h}_{\phi_{j_0,l}} = \frac{1}{N}\sum_{n=1}^{N}\phi_{j_0,l}(x_{1n}) - \frac{1}{N}\sum_{n=1}^{N}\phi_{j_0,l}(x_{2n}) \tag{30}$$

$$\hat{h}_{\psi_{j,l}} = \frac{1}{N}\sum_{n=1}^{N}\psi_{j,l}(x_{1n}) - \frac{1}{N}\sum_{n=1}^{N}\psi_{j,l}(x_{2n}). \tag{31}$$

Korišćenjem ovih rezultata izvođenja (30) i (31), optimizacioni problemi (23) i (24) se mogu zapisati u zatvorenoj formi kao:

$$\boldsymbol{\alpha}^* = \hat{\mathbf{h}}_{\Phi} \quad \text{i} \quad \boldsymbol{\beta}_j^* = \hat{\mathbf{h}}_{\Psi_j}. \tag{32}$$

Dakle, estimacija razlike funkcije gustine vjerovatnoće signala, $\hat{\mathbf{g}} \in \mathbb{R}^{N\times 1}$, se može izračunati kao:

$$\hat{\mathbf{g}} = \Phi^T\hat{\mathbf{h}}_{\Phi} + \sum_{j=j_0}^{J}\Psi^T\hat{\mathbf{h}}_{\Psi_j}. \tag{33}$$

Detekcija promjene funkcije gustine vjerovatnoće signala se vrši računanjem $L2$ mjere između estimacija funkcije gustine vjerovatnoće signala u dva vremenska intervala, odnosno, ova $L2$ mjera je $d_{L2} = \hat{\mathbf{g}}^T\hat{\mathbf{g}}$. Nakon primjene (33) se može zapisati kao:

$$d_{L2} = \hat{\mathbf{h}}_{\Phi}^T\hat{\mathbf{h}}_{\Phi} + \sum_{j=j_0}^{J}\hat{\mathbf{h}}_{\Psi_j}^T\hat{\mathbf{h}}_{\Psi_j}. \tag{34}$$

Kako su koeficijenti $\boldsymbol{\alpha}$ i $\boldsymbol{\beta}$ u (15) definisani kao srednje vrijednosti matične i skalirane *Wavelet* funkcije prozora, respektivno, $\hat{\mathbf{h}}_{\Phi}$ iz (28) se može zapisati kao $\hat{\mathbf{h}}_{\Phi} = \boldsymbol{\alpha}_1 - \boldsymbol{\alpha}_2$, dok se $\hat{\mathbf{h}}_{\Psi_j}$ iz (29) može zapisati kao $\hat{\mathbf{h}}_{\Psi_j} = \boldsymbol{\beta}_{1,j} - \boldsymbol{\beta}_{2,j}$. U ovim formulama

su $\boldsymbol{\alpha}_1$ i $\boldsymbol{\beta}_{1,j}$ *Wavlet* koeficijenti računati na intervalu $\{x_{1n}\}_{n=1}^{N}$ posmatranog signala, dok su $\boldsymbol{\alpha}_2$ i $\boldsymbol{\beta}_{2,j}$ *Wavelet* koeficijenti računati na intervalu $\{x_{2n}\}_{n=1}^{N}$.

Konačno, $L2$ mjera između distribucija signala u dva odvojena vremenska intervala, d_{L2}, se može izračunati korišćenjem isključivo *Wavelet* koeficijenata računatih na tim intervalima u obliku:

$$d_{L2} = (\boldsymbol{\alpha}_1 - \boldsymbol{\alpha}_2)^T(\boldsymbol{\alpha}_1 - \boldsymbol{\alpha}_2) + \sum_j (\boldsymbol{\beta}_{1,j} - \boldsymbol{\beta}_{2,j})^T(\boldsymbol{\beta}_{1,j} - \boldsymbol{\beta}_{2,1}). \tag{35}$$

Prilikom detekcije funkcije gustine vjerovatnoće signala potrebno je samo estimirati *Wavelet* koeficijente $\boldsymbol{\alpha}$ i $\boldsymbol{\beta}$. Ovim se izbjegava se eksplicitno estimiranje funkcije gustine vjerovatnoće signala i time smanjuje računska složenost.

Kako bi se mogla detektovati promjena funkcije gustine vjerovatnoće signala u realnom vremenu, potrebno je omogućiti računanje ovih *Wavelet* koeficijenata nad nekim nepoznatim nadolazećim signalom. Ovo se može učiniti korišćenjem *Garcia-Treviño* metoda, [8], [7].

3.5 Garcia-Treviño metod analize nadolazećeg signala

U signalima koji imaju veliki broj odbiraka, nadolazeći odbirci signala imaju manji uticaj na aproksimaciju funkcije gustine vjerovatnoće signala u odnosu na odbirke koji su ranije obrađeni, odnosno koje je prozorna funkcija ranije obuhvatila. Zbog toga je važno regulisati uticaj starih odbiraka signala na estimaciju i povećati uticaj nadolazećih odbiraka, kako bi se promjena funkcije gustine vjerovatnoće signala mogla pravovremeno detektovati. Korišćenje Garcia - Treviño metoda, opisanog u radu [8], omogućava umanjivanje uticaja starih odbiraka signala, odnosno onih koji su već prošli kroz funkciju prozora, kako bi novi, do sada neviđeni, odbirci imali veći uticaj na estimaciju. Ovakav pristup je od velikog značaja za pravovremenu detekciju promjene funkcije gustine vjerovatnoće signala.

Opisani metod se definiše sljedećim izrazom:

$$\hat{c}_{j,l}^{n} = \hat{c}_{j,l}^{n-1} + \hat{c}_{j,l}^{n,+} - \hat{c}_{j,l}^{n,-} \tag{36}$$

gdje svako $\hat{c}$ predstavlja skaliranu *Wavelet* funkciju, $\phi_{j_0,l}$, ili matičnu *Wavelet* funkciju prozora, $\psi_{j,l}$, u zavisnosti od toga da li je u pitanju α ili β koeficijent iz (35), a koji su prvenstveno definisani u (15).

$\hat{c}_{j,l}^{n,+}$ i $\hat{c}_{j,l}^{n,-}$ predstavljaju vrijednosti koje treba dodati, odnosno, oduzeti prilikom računanja novih koeficijenata, kako bismo povećali uticaj novih podataka, u odnosu

na one koji su već obrađeni. Njihove vrijednosti su:

$$\hat{c}_{j,l}^{n,+} = \begin{cases} \frac{\theta_{j,l}(x_n)}{N_w} & 2^j l \leq x_n \leq 2^j(l+2P-1), \\ 0 & \text{drugdje}, \end{cases} \tag{37}$$

$$\hat{c}_{j,l}^{n,-} = \begin{cases} \frac{\theta_{j,l}(x_n - N_w)}{N_w} & 2^j l \leq x_n - N_w \leq 2^j(l+2P-1), \\ 0 & \text{drugdje}. \end{cases} \tag{38}$$

gdje $\theta_{j,l}(x)$ predstavlja matičnu *Wavelet* funkciju prozora u slučaju računanja koeficijenta α, a u slučaju računanja koeficijenta β predstavlja skaliranu *Wavelet* funkciju prozora. N_w je širina prozora kojima se obrađuje signal, l je broj translacije odgovarajuće *Wavelet* funkcije prozora, a P rang (engl *rank*) *Wavelet* funkcije. Rang *Wavelet* funkcije predstavlja broj nultih momenata, i opisuje red polinoma funkcije koja može biti ovom *Wavelet* funkcijom prozora estimirana.

Korišćenje opisanog Garcia-Treviño metoda, obezbjeđuje uslove za veći uticaj novih odbiraka na promjenu koeficijenata α i β, u odnosu na stare, već obrađene, odbirke signala, što omogućava brzu, efikasnu i memorijski nezahtjevnu detekciju u realnom vremenu. Samim tim, može imati široku upotrebu kako u kompjuterskim naukama tako i u industrijskom sektoru.

4 GPS *spoofing* napadi

U savremenim elektroenergetskim sistemima, tačnost i pouzdanost mjerenja parametara elektroenergetskog sistema predstavljaju ključne faktore za efikasno upravljanje, zaštitu i stabilnost mreže, što iziskuje razvoj i upotrebu naprednih tehnologija za monitoring i zaštitu eletroenergetskog sistema. Međutim, pojava savremenih tehnologija, a prije svega sistema naprednih karakteristika sa većim procesorskim i memorijskim kapacitetima, kao i vještačke inteligencije i mašinskog učenja, otvara prostor za pojavu različitih sajber napada koji mogu dovesti do destabilizacije ili potpunog isključenja sistema, a samim tim i do ozbiljnih ekonomskih i materijalnih troškova.

GPS *spoofing* napade interesantnim čini to što se mogu jednostavno i jeftino realizovati korišćenjem osnovnih elektronskih komponenti, a njihova posljedica može biti destabilizacija čitavog elektroenergetskog sistema.

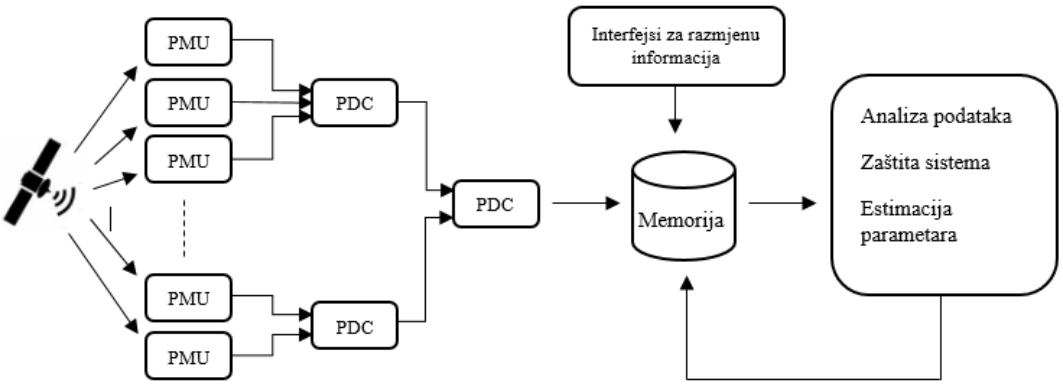
4.1 Jedinice za sinhronizovano mjerenje fazora

U analizi rada elektrodistributivnih sistema, praćenje fazora – kompleksne veličine koja opisuje sinusoidalnu funkciju u stacionarnom režimu, definisane amplitudom i faznim uglom u odnosu na referentni signal – omogućava dobijanje pravovremenih i pouzdanih informacija o stvarnom stanju napona i struja u sistemu. Jedinice za sinhronizovano mjerenje fazora predstavljaju napredne digitalne mjerne uređaje koji, za razliku od konvencionalnih mjernih instrumenata, omogućavaju simultano mjerenje efektivnih vrijednosti i faznih uglova struja i napona u elektroenergetskom sistemu.

Rad jedinica za sinhronizovano mjerenje fazora podrazumijeva mjerenje naponskog ili strujnog signala, procjenu parametara definisanog fazorskog modela i precizno određivanje trenutka kada je mjerenje izvršeno. Primjer jedinice za sinhronizovano mjerenje fazora je dat na slici 9.

Slika 9: Jedinica za sinhronizovano mjerenje fazora [34]

Jedinice za sinhronizovano mjerenje fazora predstavljaju osnovnu komponentu savremenih sistema za fazorsko praćenje (eng. *WAMS - Wide Area Measurement System*), i pravovremeno prikupljanje informacija o elektroenergetskom sistemu i njegovu analizu [35]. Šema ove infrastrukture je data na slici 10. Podaci prikupljeni na jedinicama za sinhronizovano mjerenje fazora se prosljeđuju koncentratoru (*PDC - Phasor Data Concentrator*) koji prikuplja informacije o mjerenjima, analizira ih, a istovremeno dobija i informaciju o vremenskom trenutku mjerenja. Njegov zadatak je da prikuplja, sortira i grupiše mjerenja napona i struje sa jedinica za sinhronizovano mjerenje fazora po njihovom vremenskom žigu (eng. *timestamp*) i time omogućava autentičnu rekonstrukciju stanja sistema u određenom trenutku.



Slika 10: Šema infrastrukture sistema za fazorsko praćenje, po ugledu na [36]

Sa koncentratora se prikupljene i analizirane informacije arhiviraju u memoriju

i kasnije se mogu koristiti za upravljanje, analizu i zaštitu kompletnog elektroenergetskog sistema.

4.2 GPS sinhronizacija uređaja za mjerenje fazora

Da bi se osigurala tačnost i upotrebljivost fazorskih mjerenja koja dolaze iz različitih mjernih jedinica, neophodno je da svi fazori budu izračunati u odnosu na isti referentni signal. U okviru savremenih sistema za praćenje fazora, sinhronizacija fazorskih mjernih jedinica se postiže korišćenjem globalnog pozicionog sistema (GPS), koji pruža zajednički referentni signal.

GPS sistem, koji se sastoji od 24 satelita u Zemljinoj orbiti, obezbjeđuje visoko precizne vremenske podatke putem svojih atomskih časovnika. Da bi odredili tačnu poziciju, GPS prijemnici dekodiraju signale sa najmanje četiri satelita i sinhronizuju se sa atomskim časovnicima koji se nalaze u tim satelitima. Na osnovu određene pozicije i sinhronizacije sa atomskim časovnicima, GPS prijemnici mogu tačno odrediti i vrijeme.

Prema **IEEE/IEC 60255-118** standardu, GPS prijemnici korišćeni u savremenim fazorskim mjernim jedinicama moraju osigurati vremensku grešku manju od 1 μs, [37]. Međutim, u praksi su fazorska mjerenja obično sinhronizovana sa greškom manjom od 0.1 μs [38], što, posmatrano kroz fazni stav, koji se računa kao $\Delta\theta = 360° \cdot f \cdot \Delta t$ (f - frekvencija sistema, Δt - vremensko kašnjenje), rezultira greškom manjom od 0.018° za sisteme sa nominalnom frekvencijom od 50 Hz.

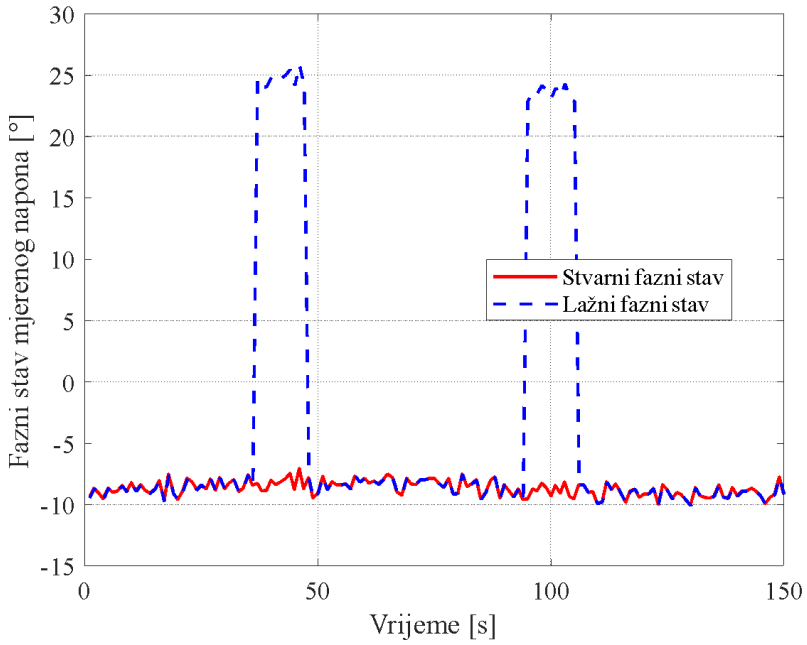
4.2.1 GPS *spoofing* napadi

Civilni GPS prijemnici koji se koriste u uređajima za sinhronizovano mjerenje fazora ne koriste enkripciju, što ih čini ranjivim na razne vrste sajber napada koji mogu dovesti do isključenja sistema i izazvati ozbilje socio-ekonomske reperkusije. Jedna vrsta takvih sajber napada su i GPS *spoofing* napadi, tokom kojih napadač emituje lažni GPS signal koji oponaša autentični signal. Kako se snaga lažnog signala postepeno povećava, GPS prijemnik preusmjerava praćenje na lažni signal, što dovodi do netačne vremenske sinhronizacije i grešaka u mjerenju, a ovi napadi se mogu realizovati korišćenjem osnovnih elektronskih komponenti [39].

Greške u vremenskoj sinhronizaciji direktno se manifestuju kroz fazne pomake u svim mjerenjima uređaja za sinhronizovano mjerenje fazora.

Na slici 11 prikazan je signal sa uređaja pogođenog GPS *spoofing* napadima tokom perioda od 150 sekundi, pri čemu su napadi uzrokovali fazne pomake, odnosno

promjenu faznog stava napona u trenucima napada.



Slika 11: Primjer efekata napada lažiranjem GPS signala na uređaj za sinhronizovano mjerenje fazora. Puna linija predstavlja stvarni fazni stav napona, dok isprekidana linija predstavlja lažni fazni stav napona koji se detektuje

Iako su u ovom primjeru napadi lako uočljivi, sofisticiraniji napadi mogu izazvati suptilnije promjene koje oponašaju prirodne fluktuacije u sistemu, što otežava detekciju. Stoga, razvoj metoda za detekciju GPS *spoofing* napada predstavlja ključni izazov u kontekstu sajber bezbjednosti elektroenergetskih sistema. Ovo naglašava značaj sinhronizacije i sigurnosti u radu savremenih elektroenergetskih sistema, s posebnim fokusom na prijetnje poput GPS *spoofing* napada, koje mogu ozbiljno narušiti tačnost i pouzdanost fazorskih mjerenja.

5 Primjena algoritma detekcije promjene distribucije signala na identifikaciju GPS *spoofing* napada

Mjerenja koja jedinice za sinhronizovano mjerenje fazora dostavljaju, nakon obrade unutar jedinice, predstavljaju fazore strujnog i naponskog stanja. Mjerenja se obavljaju u fiksnim vremenskim razmacima. Sva mjerenja sa jednog uređaja se mogu konkatenirati i posmatrati kao odbirci kontinualnog signala. Tačnije, u svakom trenutku se mjere amplituda i fazni ugao napona, kao i amplituda i fazni ugao struje za svaku mjerenu fazu. Ako se pretpostavi da je prvo mjerenje monofazno, veličine se mogu zapisati kao $[|V_1|, \theta_{V_1}, |I_1|, \theta_{I_1}]$, gdje su $|V_1|$ i $|I_1|$ amplitude napona i struje, a θ_{V_1} i θ_{I_1} fazni uglovi napona i struje respektivno. Za n ovakvih mjerenja, konkatenirani signal će imati oblik: $[|V_1|, \theta_{V_1}, |I_1|\theta_{I_1}, ..., |V_n|, \theta_{V_n}, |I_n|, \theta_{I_n}]$. U praksi ovaj signal ima neku kontinualnu funkciju gustine vjerovatnoće signala.

GPS *spoofing* napadi, opisani u 4.2.1, se realizuju slanjem lažnog GPS signala jedinicama za sinhronizovano mjerenje fazora i time unose fazni pomak u sva mjerenja na kompromitovanom uređaju. Ovo znači da će, prilikom GPS *spoofing* napada, doći do promjene funkcije gustine vjerovatnoće signala dobijenog nadovezivanjem vrijednosti izmjerenih na napadnutoj jedinici. Navedeno je osnov za korišćenje statističkih metoda za detekciju funkcije gustine vjerovatnoće signala u cilju identifikacije GPS *spoofing* napada na jedinice za sinhronizovano mjerenje fazora.

U slučaju identifikacije GPS *spoofing* napada metodom detekcije promjene funkcije gustine vjerovatnoće signala računa se vrijednost $L2$ mjere između koeficijenata *Wavelet* razvoja distribucije signala dobijenih u toku dva odvojena vremenska intervala. GPS **spoofing** napad se proglašava u trenutku kada ova $L2$ mjera bude veća od predefinisane referentne vrijednosti praga, kako je objašnjeno u podsekciji 3.4.

Predloženi metod identifikacije GPS *spoofing* napada ne iziskuje velike memorijske zahtjeve niti natprosječnu procesorsku moć što ga izdvaja u odnosu na druge metode detekcije koje zahtijevaju složene hardverske komponente ili skupe procesorske jedinice, kakve su metode mašinskog učenja i vještačke inteligencije [19].

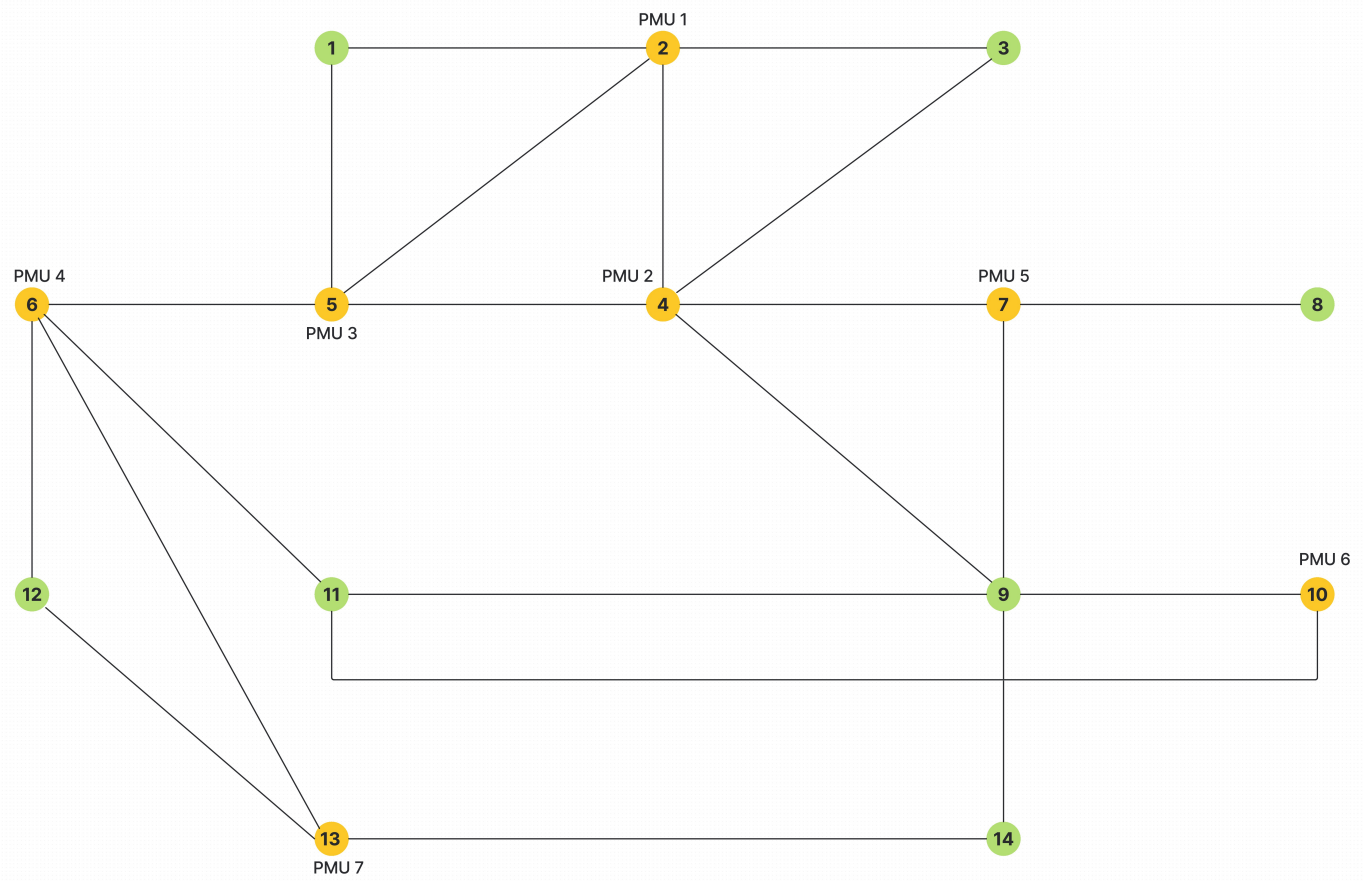
6 Opis eksperimentalne metodologije

Uzimajući u obzir činjenicu da su svi istraživački eksperimenti na elektroenergetskim sistemima zabranjeni, kao i visoke cijene uređaja za sinhronizovano mjerenje fazora, ustaljena istraživačka praksa je da se svi eksperimenti u oblasti sajber bezbjednosti elektroenergetskih sistema i njegovih komponenti vrše u simulacionom okruženju [12]. Stoga su i istraživanja primjene algoritma za detekciju funkcije gustine vjerovatnoće signala u cilju identifikacije GPS *spoofing* napada vršena u okruženjima **MATLAB** i **Python**.

6.1 Set podataka

U simulacionom okruženju, sintetička fazorska mjerenja su generisana sprovođenjem proračuna tokova snaga na testnom elektroenergetskom sistemu od **14** čvorova (eng. *IEEE* 14-*bus test system*), **57** čvorova (eng. *IEEE* 57-*bus test system*) i **118** čvorova (eng. *IEEE* 118-*bus test system*), pri čemu je mjerna konfiguracija definisana tako da obezbjeđuje opservabilnost posmatranog sistema uz minimalan broj uređaja za sinhronizovano mjerenje fazora, [40]. Tako je u eksperimentima u kojima je korišćeno 14 čvorova prisutno **7** jedinica za sinhronizovano mjernje fazora. Uloga svake od ovih jedinica je da posmatra stanje napona u susjednim čvorovima i stanje struje u povezanim granama. Optimalno praćenje željenih veličina se može postići i sa manjim brojem jedinica, međutim, veći broj jedinica za sinhronizovano mjerenje fazora umanjuje mogućnost pojave nedetektovanih sajber napada. Poštujući ovaj princip, u eksperimentima u kojima se posmatra 57 čvorova prisutno je **17** jedinica za mjerenje fazora, dok su u slučaju praćenja stanja u sistemu sa 118 čvorova prisutne **32** jedinice za sinhronizovano mjerenje fazora.

U slučaju eksperimenata sa 7 jedinica za sinhronizovano mjerenje fazora (14 čvorova) set jednovremenih mjernih podataka čine 32 fazorska mjerenja. Sistem koji je korišćen u eksperimentima je prikazan na slici 12.



Slika 12: Shema 14-čvornog sistema sa 7 jedinica za sinhronizovano mjerenje fazora

Pošto svaka jedinica za sinhronizovano mjerenje fazora posmatra napon na sopstvenom čvoru i struje u granama koje su priključene na taj čvor, može se zaključiti da, npr. prva jedinica (PMU 1) mjeri amplitudu i fazni stav napona na čvoru broj 2, kao i amplitudu i fazni stav struja u granama prema susjednim čvorovima odnosno, 1, 3, 4 i 5. Što je ukupno 5 fazorskih mjerenja, odnosno dobija se 10 vrijednosti. Tako ostale jedinice računaju:

- PMU 2: amplitudu i fazni stav napona na čvoru 4, kao i amplitude i fazne stavove struja u granama prema čvorovima 2, 3, 5, 7 i 9, odnosno 6 fazorskih mjerenja (12 vrijednosti);
- PMU 3: amplitudu i fazni stav napona na čvoru 5, kao i amplitude i fazne stavove struja prema čvorovima 1, 2, 4 i 6, odnosno 5 fazorskih mjerenja (10 vrijednosti);
- PMU 4: amplitudu i fazni stav napona na čvoru 6, kao i amplitude i fazne stavove struja u prema čvorovima 5, 11, 12 i 13, što broji 5 fazorskih mjerenja (10 vrijednosti);

- PMU 5: amplitudu i fazni stav napona na čvoru 7, kao i amplitude i fazne stavove struja prema čvorovima 4, 8 i 9, odnosno 4 fazorska mjerenja (8 vrijednosti);
- PMU 6: amplitudu i fazni stav napona na čvoru 10, kao i amplitude i fazne stavove struja prema čvorovima 9 i 11, odnosno 3 fazorska mjerenja (6 vrijednosti);
- PMU 7: amplitudu i fazni stav napona na čvoru 13, kao i amplitude i fazne stavove struja prema čvorovima 6, 12 i 14, odnosno 4 fazorska mjerenja (8 vrijednosti).

Na osnovu ove računice dolazi se do zaključka da jedno istovremeno mjerenje na svim jedinicama za sinhronizovano mjerenje daje ukupno 32 fazorska mjerenja, odnosno 64 vrijednosti.

Slično kao u prethodnom primjeru, u slučaju seta od 17 jedinica za sinhronizovano mjerenje fazora, u jednom trenutku se računa 138 fazorskih mjerenja, a u slučaju seta od 32 jedinice za sinhronizovano mjerenje fazora 168 fazorskih mjerenja struja i napona.

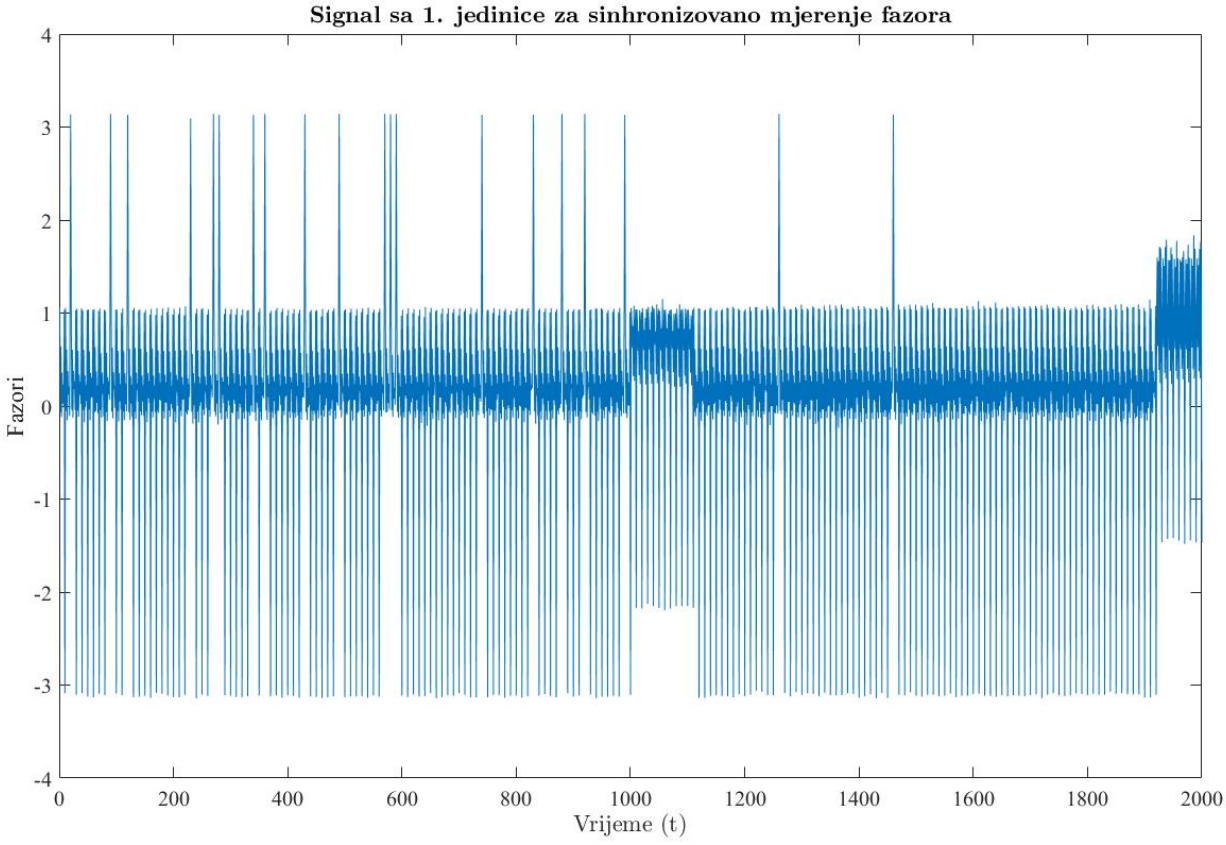
Radi simulacije prisustva slučajnih mjernih odstupanja, svim fazorskim mjerenjima je dodat aditivni mjerni šum modelovan Gausovom (normalnom) raspodjelom sa standardnom devijacijom $\sigma = 0.01$. Ovakav pristup predstavlja uobičajeni metod za modelovanje slučajnih mjernih grešaka u elektroenergetskim sistemima [12].

GPS *spoofing* napadi simulirani su modifikovanjem faznih stavova svih mjerenja, različitim vrijednostima u opsegu od 0° do 150°, u slučajno odabranim trenucima, kao i na slučajno odabranim jedinicama. U toku generisanja ovih signala čuvaju se informacije o vremenskom trenutku mjerenja tokom kojih je izvršena izmjena faznog stava kako bi se mogla utvrditi tačnost i preciznost algoritma. Izloženom procedurom su generisana fazorska mjerenja struja i napona u 10,000 trenutaka, u svakom od pomenutih sistema.

U cilju identifikacije GPS *spoofing* napada koriste se signali generisani na jedinicama za sinhronizovano mjerenje fazora, a mjerenja na svakoj od jedinica se posmatraju zasebno. Analizirani signal se dobija konkatenacijom više uzastopnih mjerenja na jednoj jedinici i na njemu se očekuje nepromjenljiva funkcija gustine vjerovatnoće signala.

Za potrebe ovog eksperimenta korišćeno je **200** uzastopnih mjerenja kako bi se smanjio obim računa budući da se detekcija može izvršiti nakon samo jednog

mjerenja za koje se pretpostavlja da nije podvrgnuto GPS *spoofing* napadu. Primjer signala sa jedne od stanica je prikazan na slici 13.



Slika 13: Signal sa jedinice za sinhronizovano mjerenje fazora

Na slici je prikazan signal sa prve jedinice za sinhronizovano mjerenje fazora. Konkatenirane su vrijednosti sa 200 uzastopnih mjerenja, i time dobijen signal dužine 2000 odbiraka. Uočljivo je da funkcija gustine vjerovatnoće signala ima iste parametre, srednju vrijednost i varijansu do 1002. odbirka, gdje dolazi do nagle promjene u ovim vrijednostima i samim tim u funkciji gustine vjerovatnoće signala. Pošto na prvoj stanici jedno mjerenje daje signal od 10 vrijednosti, odnosno 5 fazorskih mjerenja, može se zaključiti da je promjena nastala u trenutku 101. mjerenja. Signal ponovo dostiže prvobitnu srednju vrijednost i varijansu u trenutku 1111. odbirka, odnosno u trenutku 112. mjerenja. Dakle, promjene funkcije gustine vjerovatnoće signala je trajala 10 mjerenja i detektovana je već u prvom mjerenju. Slična situacija se događa i u trenutku 1922. odbirka, odnosno 193. mjerenja. Ove nagle promjene u srednjoj vrijednosti signala, samim tim i u funkciji gustine vjerovatnoće signala, predstavljaju signal u trenucima GPS *spoofing* napada.

6.2 Eksperimentalni postupak i rezultati detekcije promjene funkcije gustine vjerovatnoće signala u cilju identifikacije GPS *spoofing* napada

U ovoj sekciji su izloženi rezultati primjene predložene detekcije na prethodno opisanim signalima. Korišćena su dva prozora jednake širine za analizu signala. Referentni prozor obuhvata segment signala iz prvog mjerenja, čiji *Wavelet* koeficijenti implicitno sadrže informaciju o funkciji gustine vjerovatnoće. Iako se funkcija gustine vjerovatnoće signala ne procjenjuje direktno, raspodjela ovih koeficijenata koristi se kao referentna u postupku detekcije promjene. Ovo je učinjeno pod pretpostavkom da će se u praksi signal posmatrati i prije samog početka napada. Drugi prozor obuhvata dio nadolazećeg signala, a u praktičnoj primjeni to će biti nepoznati signal. Početna pozicija drugog prozora je takva da obuhvata prvi odbirak nakon dijela signala koji je obuhvaćen referentnim prozorom i obuhvatiće jednak broj odbiraka kao i referentni prozor.

Širine oba prozora diktira broj vrijednosti koje se dobiju u toku jednog mjerenja. Ove vrijednosti širina zavisiće od topologije mreže, a biće jednake dvostrukoj vrijednosti broja fazorskih mjerenja koje računa ta jedinica [41].

Poseban fokus u toku istraživanja je dat izboru *Wavelet* porodice kojom će se vršiti računanje *Wavelet* koeficijenata kao i odluci o korišćenju skalirane *Wavelet* funkcije prozora u procesu ažuriranja parametara.

Algoritam prati sljedeće korake:

1. Definisanje početnih vrijednosti *Wavelet* koeficijenata, ove vrijednosti mogu biti nule, jedinice ili neke slučajno odabrane vrijednosti. U eksperimentima identifikacije GPS *spoofing* napada metodom detekcije promjene funkcije gustine vjerovatnoće signala se za početne vrijednosti koeficijenata koriste nule.

2. Analiziranje signala prozorima. Referentni prozor ostaje „fiksiran“, dok se drugim, pomjerajućim prozorom, analizira ostatak signala, odnosno moguća promjena funkcije gustine vjerovatnoće signala. U toku ovog postupka se ne dekomponuje cijeli signal *Wavelet* transformacijom, već se koeficijenti *Wavelet* transformacije, α i β, ažuriraju korišćenjem *Garcia Treviño* metode, opisane u 3.5.

3. Računanje $L2$ mjere između koeficijenata dobijenih u referentnom i pomjerajućem prozoru.

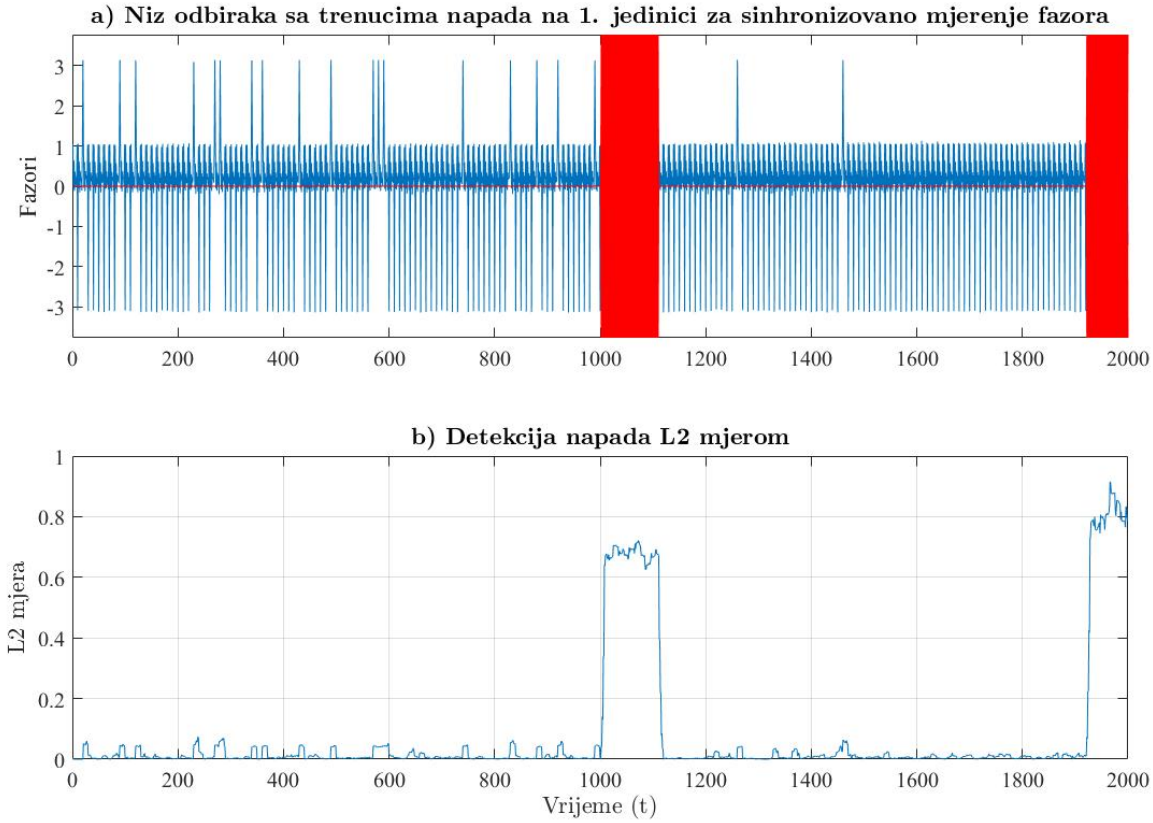
4. Proglašavanje početka GPS *spoofing* napada u trenutku kada vrijednost $L2$ mjere bude veća od predefinisane referentne vrijednosti praga.

6.2.1 Rezultati detekcije promjene funkcije gustine vjerovatnoće signala računanjem $L2$ mjere između *Wavelet* koeficijenata distribucije signala

Detekcija promjene funkcije gustine vjerovatnoće signala zasnovana je na praćenju promjena $L2$ mjere računate između *Wavelet* koeficijenata dijela signala u referentnom prozoru i *Wavelet* koeficijenata dijela signala u pomjerajućem prozoru u datom trenutku vremena. Što je vrijednost $L2$ mjere veća, smatra se da je algoritam sigurniji da u datom trenutku dolazi do promjene funkcije gustine vjerovatnoće signala, odnosno, mjera sličnosti između dva dijela signala pokazuje da postoji promjena. U tom trenutku se proglašava početak GPS *spoofing* napada.

U nastavku će, zbog jednostavnosti prikaza, biti predstavljene performanse algoritma na jednom setu simuliranih mjerenja sistema od 14 čvorova, odnosno, 7 jedinica.

Na slici 14 predstavljena je detekcija promjene funkcije gustine vjerovatnoće na 1. jedinici za sinhronizovano mjerenje fazora (PMU 1). Na grafiku a) predstavljen je originalni signal. Crvenom bojom su označeni odbirci na kojima je dodat fazni pomak, odnosno, koji su pod GPS *spoofing* napadom. Na slici 14 b) je predstavljena detekcija promjene funkcije gustine vjerovatnoće naglom promjenom $L2$ mjere, po postupku opisanom u sekciji 6.2.



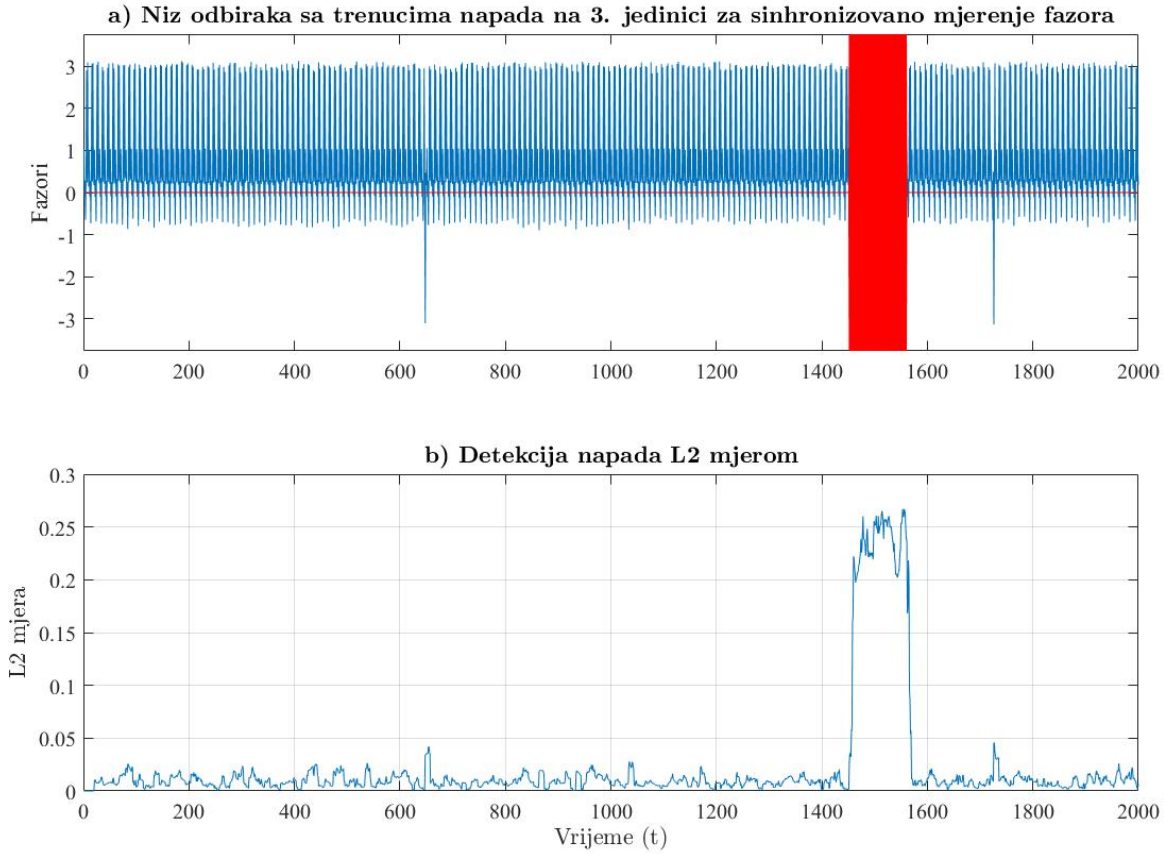
Slika 14: Detekcija promjene distribucije signala na 1. jedinici za sinhronizovano mjerenje fazora: a) pozicije stvarnih GPS *spoofing* napada obilježene crvenom bojom, b) L2 mjera računata između *Wavelet* koeficijenata dijela signala u referentnom prozoru i dijela signala u klizećem prozoru, pozicije sa značajno većim vrijednostima predstavljaju detektovane GPS *spoofing* napade

Na slici 14 se može primijetiti da je došlo do nagle promjene $L2$ mjere i da je metod uspješno detektovao promjenu funkcije gustine vjerovatnoće ovog signala. Stvarna promjena funkcije gustine vjerovatnoće signala nastala je u momentu **1002.** odbirka, odnosno fazora, dok je promjena funkcije gustine vjerovatnoće signala detektovana već u momentu **1006.** odbirka, što se iskazuje naglim porastom vrijednosti $L2$ mjere u trenucima ovih odbiraka. Dakle, kašnjenje detekcije iznosi **4** odbirka, odnosno fazora. Uzimajući u obzir da jedno mjerenje sadrži 10 fazora u slučaju 1. jedinice za sinhronizovano mjerenje fazora sistema od 14 čvorova, ovo znači da će napad biti detektovan već u prvom mjerenju u kom je došlo do promjene faznog stava, odnosno, do GPS *spoofing* napada.

Može se primijetiti nagla promjena $L2$ mjere, odnosno promjena funkcije gustine vjerovatnoće signala u trenutku **1926.** odbirka. Stvarna promjena funkcije gustine vjerovatnoće signala dešava se na **1922.** odbirku, što ukazuje na kašnjenje detekcije

od samo **4** odbirka, odnosno fazorska mjerenja. S obzirom na to da u toku simulacije jednog fazorskog mjerenja jedinica dostavlja 10 vrijednosti, zaključuje se da je napad detektovan u toku prvog mjerenja na kom je došlo do promjene faznog stava.

Još jedan primjer uspješne detekcije prikazan je na slici 15. Slika prikazuje fazorska mjerenja sa 3. jedinice za sinhronizovano mjerenje fazora sistema od 14 čvorova, odnosno, 7 jedinica. Signal obuhvata 200 setova jednovremenih fazorskih mjerenja sa 3. jedinice. Na slici 15, na grafiku a) su prikazane pozicije fazora na kojima je došlo do promjene faznog stava, dok je na grafiku b) prikazana detekcija promjene funkcije gustine vjerovatnoće signala $L2$ mjerom.



Slika 15: Detekcija promjene distribucije signala na 3. jedinici za sinhronizovano mjerenje fazora: a) pozicije stvarnih GPS *spoofing* napada obilježene crvenom bojom, b) L2 mjera računata između *Wavelet* koeficijenata dijela signala u referentnom prozoru i dijela signala u klizećem prozoru, pozicije sa značajno većim vrijednostima predstavljaju detektovane GPS *spoofing* napade

Na slici 15 se uočava da je promjena funkcije gustine vjerovatnoće signala detektovana na **1460.** fazoru, dok se stvarna promjena dogodila u momentu **1452.** fazora.

Kao i u slučaju 1. jedinice za sinhronizovano mjerenje fazora, set koji simulira fazorska mjerenja sa 3. jedinice sadrži 10 vrijednosti, što znači da je napad detektovan nakon samo **8** fazora, odnosno, u toku mjerenja u kom je došlo do stvarne promjene.

Rezultati eksperimenata upoređivani su sa drugim metodama detekcije promjene funkcije gustine vjerovatnoće signala, i to mjerom maksimalne vjerovatnoće između estimacija funkcije gustine vjerovatnoće signala i računanjem relativne entropije između estimacija funkcije gustine vjerovatnoće signala u referentnom i pomjerajućem prozoru. Ovi postupci detaljnije su opisani u sekciji 3 i podsekcijama 3.2 i 3.3. Sama estimacija funkcija gustine vjerovatnoće signala u prozorima se takođe vrši na dva načina: estimacija histogramom, objašnjena u podsekciji 3.1 i pretpostavljanjem Gausove raspodjele i estimiranjem njenih parametara i vrše se nad signalom istog seta mjerenja nad kojem je računata i $L2$ mjera. Rezultati su prezentovani na sistemu od 14 čvorova, 7 jedinica, na jedinicama 1 i 3.

Na slici16 je prikazano poređenje algoritma detekcije promjene funkcije gustine vjerovatnoće signala računanjem $L2$ mjere između koeficijenata *Wavelet* razvoja sa metodama koje računaju mjeru maksimalne vjerovatnoće i relativnu entropiju između estimacija funkcija gustine vjerovatnoće.

Na slici 16, grafiku a) predstavljeni su odbirci signala, dok su crvenom bojom obilježeni fazori kojima je dodat fazni pomak, odnosno, koji su pod GPS *spoofing* napadom. Stvarne promjene funkcije gustine vjerovatnoće signala nastaju na **1002.** fazoru i na **1922.** fazoru. Na slici 16, na grafiku b) predstavljena je detekcija promjene distribucije signala $L2$ mjerom i kao i u prethodnom primjeru uočljiva je uspješna i brza detekcija.

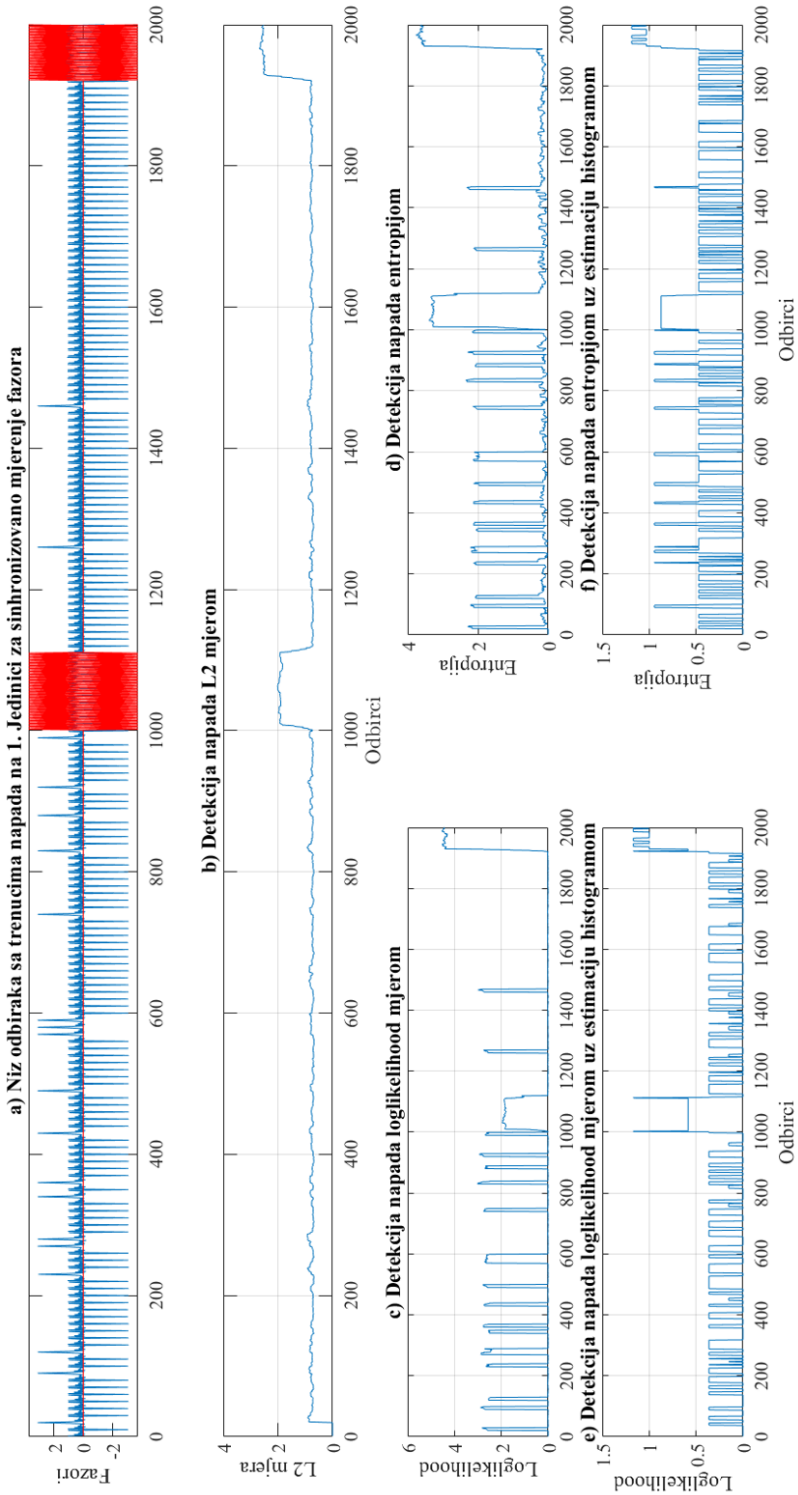
Na slici 16, na graficima c) i e) predstavljena je detekcija promjene funkcije gustine vjerovatnoće signala računanjem mjere maksimalne vjerovatnoće između procijenjenih distribucija signala dobijenih u dva prozora. Na grafiku c) je predstavljen slučaj kada se za estimaciju funkcije gustine vjerovatnoće signala pretpostavlja Gausova raspodjela signala i estimiraju njeni parametri, dok je na grafiku e) predstavljen slučaj kada se za funkciju gustine vjerovatnoće signala koristi estimacija histogramom.

U slučaju detekcije promjene funkcije gustine vjerovatnoće signala metodom procjene maksimalne vjerovatnoće, promjena je detektovana na **1002.** fazoru i **1922.** fazoru, što znači da je brzina detekcije bolja od detekcije $L2$ mjerom. Međutim, kako se na slici 16, na graficima c) i e) može primijetiti kod ovog metoda, i u slučaju estimacije histogramom i estimiranjem parametara Gausove raspodjele pojavljuje se veliki broj stupaca koji predstavljaju lažne detekcije promjene funkcije gustine vjerovatnoće signala. Slična situacija se dešava i u slučaju promjene faznog stava u

momentu 1922. odbirka. To čini detekciju promjene funkcije gustine vjerovatnoće signala $L2$ mjerom stabilnijom i preciznijom u pogledu broja tačnih detekcija u odnosu na detekciju računanjem mjere maksimalne vjerovatnoće.

Na slici 16, na graficima d) i f) predstavljena je detekcija promjene funkcije gustine vjerovatnoće signala metodom zasnovanoj na računanju relativne entropije između estimacija distribucije signala. Na grafiku d) je predstavljen slučaj kada se za estimaciju funkcije gustine vjerovatnoće signala pretpostavlja bazna Gausova raspodjela i estimiraju njeni parametri, dok je na grafiku f) predstavljen slučaj kada se za estimaciju funkcije gustine vjerovatnoće signala koristi histogram.

U slučaju detekcije promjene funkcije gustine vjerovatnoće signala, promjena je detektovana tek na **1010.** fazoru i **1930.** fazoru, što znači da ima veće kašnjenje nego detekcija $L2$ mjerom koja je promjenu detektovala na **1006.** odbirku i **1026.** odbirku. Uz to, u slučaju detekcije promjene funkcije gustine vjerovatnoće signala računanjem relativne entropije prisutan je veliki broj stupaca koji predstavljaju lažne detekcije, pa je i u ovom slučaju metod detekcije $L2$ mjerom dao bolje rezultate u pogledu preciznosti, odnosno broja tačnih detekcija promjena i stabilnih perioda.



Slika 16: Detekcija promjene distribucije signala pomoću nekoliko metoda na 1. jedinici za sinhronizovano mjerenje fazora: a) pozicije stvarnih GPS *spoofing* napada obilježene crvenom bojom, b) L2 mjera računata između *Wavelet* koeficijenata dijela signala u referentnom prozoru i dijela signala u klizećem prozoru, pozicije sa značajno većim vrijednostima predstavljaju detektovane GPS *spoofing* napade, c) detekcija GPS *spoofing* napada računanjem mjere maksimalne vjerovatnoće između estimiranih funkcija gustine vjerovatnoće signala dobijenih estimiranjem parametara pretpostavljene Gausove funkcije raspodjele, d) detekcija GPS *spoofing* napada računanjem entropije između estimiranih funkcija gustine vjerovatnoće signala dobijenih estimiranjem parametara pretpostavljene Gausove funkcije raspodjele, e) detekcija GPS *spoofing* napada računanjem mjere maksimalne vjerovatnoće signala između estimiranih funkcija gustine vjerovatnoće signala dobijenih estimacijom histogramom, f) detekcija GPS *spoofing* napada računanjem entropije između estimiranih funkcija gustine vjerovatnoće signala dobijenih estimacijom historgramom

Još jedan primjer rezultata poređenja detekcije promjene funkcije gustine vjerovatnoće signala $L2$ mjerom sa drugim metodama detekcije promjene distribucije signala je prikazan na slici 17.

Na slici 17, na grafiku a) je prikazan signal sa 3. jedinice za sinhronizovano mjerenje fazora, dok su crvenom bojom predstavljene pozicije fazora koji imaju fazni pomjeraj. Na grafiku b) je predstavljena detekcija promjene funkcije gustine vjerovatnoće signala računanjem $L2$ mjere između koeficijenata *Wavelet* razvoja.

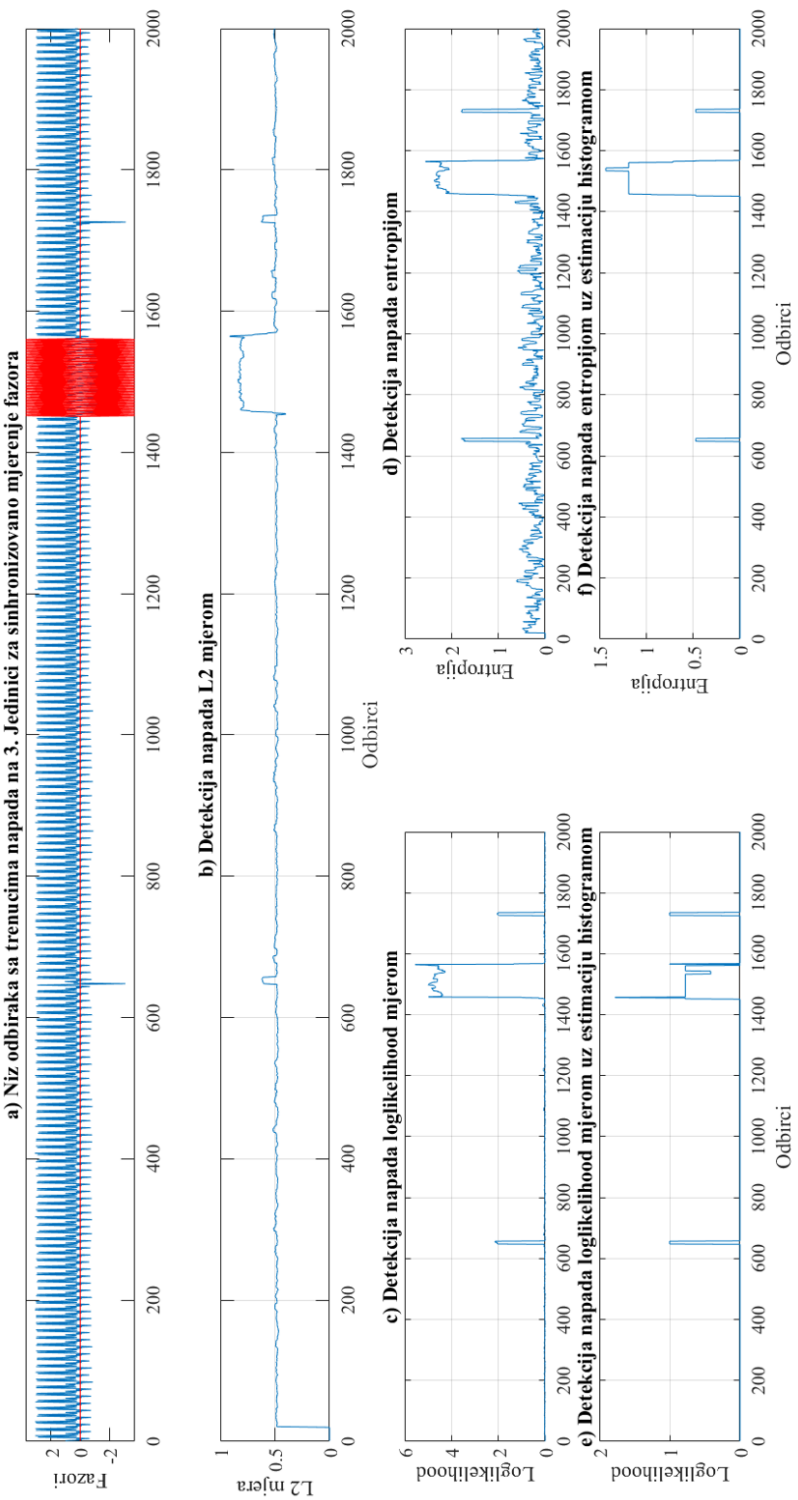
Na slici 17, na graficima c) i e) je predstavljena detekcija promjene funkcije gustine vjerovatnoće signala računanjem mjere maksimalne vjerovatnoće između estimacija distribucije signala na intervalima obuhvaćenim prozorima. Na grafiku c) je predstavljen slučaj kada se za estimaciju funkcije gustine vjerovatnoće signala pretpostavlja Gausova funkcija raspodjele signala i estimiraju njeni parametri, dok je na grafiku e) predstavljen slučaj kada se estimacija vrši korišćenjem histograma.

Promjena funkcije gustine vjerovatnoće signala u slučaju računanja mjere maksimalne vjerovatnoće je detektovana na **1456.** odbirku i vidi se da i u ovom slučaju ima bolju brzinu detekcije kao i detekcija $L2$ mjerom, međutim i da ima nekoliko lažnih detekcija detektovanih sa približno istom sigurnošću kao i stvarna promjena funkcije gustine vjerovatnoće signala.

Na slici 17, na graficima d) i f) je predstavljena detekcija promjene funkcije gustine vjerovatnoće signala računanjem entropije između estimacija funkcije gustine vjerovatnoće signala u intervalima obuhvaćenim prozorima. Na grafiku d) je predstavljen slučaj kada se za estimaciju funkcije gustine vjerovatnoće signala estimiraju parametri pretpostavljene Gausove funkcije gustine vjeorvatnoće, dok je na grafiku f) predstavljen slučaj kada se estimacija vrši histogramom.

U slučaju detekcije promjene funkcije gustine vjerovatnoće signala računanjem entropije, promjena je detektovana na **1460.** fazoru, isto kao i u slučaju detekcije računanjem $L2$ mjere. Brzina detekcije je u potpunosti ista, međutim, u slučaju detekcije entropijom pojavljuju se stupci koji predstavljaju lažne detekcije signala.

Uzevši u obzir predstavljene rezultate dolazi se do zaključka da detekcija promjene funkcije gustine vjerovatnoće signala $L2$ mjere predstavlja optimalano rješenje u pogledu brzine detekcije i tačnosti



Slika 17: Detekcija promjene distribucije signala pomoću nekoliko metoda na 3. jedinici za sinhronizovano mjerenje fazora: a) pozicije stvarnih GPS *spoofing* napada obilježene crvenom bojom, b) L2 mjera računata između *Wavelet* koeficijenata dijela signala u referentnom prozoru i dijela signala u klizećem prozoru, pozicije sa značajno većim vrijednostima predstavljaju detektovane GPS *spoofing* napade, c) detekcija GPS *spoofing* napada računanjem mjere maksimalne vjerovatnoće između estimiranih funkcija gustine vjerovatnoće signala dobijenih estimiranjem parametara pretpostavljene Gausove funkcije raspodjele, d) detekcija GPS *spoofing* napada računanjem entropije između estimiranih funkcija gustine vjerovatnoće signala dobijenih estimiranjem parametara pretpostavljene Gausove funkcije raspodjele, e) detekcija GPS *spoofing* napada računanjem mjere maksimalne vjerovatnoće signala između estimiranih funkcija gustine vjerovatnoće signala dobijenih estimacijom histogramom, f) detekcija GPS *spoofing* napada računanjem entropije između estimiranih funkcija gustine vjerovatnoće signala dobijenih estimacijom historgramom

7 Odabir parametara algoritma

U procesu analize performansi predloženog metoda posebna pažnja je posvećena odabiru odgovarajuće *Wavelet* porodice i rangu *Wavelet* transformacije, koji je u (37) i (38) označen kao **P**, a predstavlja broj nultih momenata (eng. *vanishing moments*) *Wavelet* baze. Rang *Wavelet* transformacije može uticati na red polinoma kojim se signal može predstaviti. Takođe, analiziran je uticaj skalirane *Wavelet* funkcije prozora na vrijednosti koeficijenata *Wavelet* distribucije signala i detekciju promjene funkcije gustine vjerovatnoće signala.

Eksperimenti su rađeni na signalima koji predstavljaju simulacije fazorskih mjerenja jedinica za sinhronizovano mjerenje fazora u testnim okruženjima sa 14, 57 i 118 čvorova, međutim, radi preglednosti i lakše analize rezultati će grafički biti predstavljeni na signalu koji simulira mjerenja 1. jedinice za sinhronizovano mjerenje fazora prikazanom na slici 14. U eksperimentima su korišćene funkcije prozora svih *Wavelet* porodica koje zaodovoljavaju uslov ortogonalnosti odgovarajućih rangova, kako je i opisano u narednoj podsekciji.

7.1 Analiza uticaja odabira *Wavelet* porodice na detekciju promjene funkcije gustine vjerovatnoće signala

Za potrebe ovog eksperimenta korišćene su matična i skalirana *Wavelet* funkcija prozora koje pripadaju porodicama sa ortogonalnim bazama i sa različitim vrijednostima ranga (reda *Wavelet* baze). Funkcije sa manjim brojem nultih momenata su pogodnije za detekciju naglih promjena signala i stoga su u eksperimentu korišćene funkcije nižih rangova. Funkcije koje su korišćene pripadaju:

- *Daubachies Wavelet* porodici, rangova: **2, 3, 4, 5, 6, 7, 8, 9** i **10**. Rang veličine **1** nije korišćen zato što se njime mogu reprezentovati samo funkcije konstantnih vrijednosti, što nije čest slučaj u praksi, posebno u slučaju elektroenergetskih sistema.
- *Coiflet Wavelet* porodici, rangova: **2, 3, 4** i **5**. Kao i u slučaju *Daubachies Wavelet* porodice, funkcija prozora sa rangom **1** nije korišćena jer se u praksi ne očekuje analiza signala konstantnih vrijednosti. Rangovi većeg stepena od **5** takođe nisu korišćeni jer je ustaljena istraživačka praksa pokazala da rang većeg reda usložnjava računski proces bez znantnih poboljšanja u rezultatima, [42].

- *Symlet Wavelet* porodici, rangova: **4, 5, 6, 7, 8, 9** i **10**. Razlog za korišćenje ovih rangova je taj što *Symlet Wavelet* funkcija manjeg ranga, zbog svoje glatkije prirode u odnosu na druge navedene porodice, može dobro lokalizovati nagle promjene, ali i zanemariti suptilnije promjene [43].

Rang *Wavelet* funkcije u praksi određuje dužinu takozvanog vektora nosioca (eng. *support vector*) koji ima dvostruku vrijednost ranga *Wavelet* funkcije, $2P$, i predstavlja ograničeni interval na kom je *Wavelet* funkcija različita od nule. *Haar Wavelet* transformacija je definisana intervalima konstantnih vrijednosti i upravo ta jednostavnost, izražena kroz diskontinuitete i odsustvo glatkoće funkcije, čini ovu *Wavelet* bazu neprikladnom za analizu signala koji zahtijevaju detaljniju lokalnu aproksimaciju ili interpretaciju frekvencijskog sadržaja.

U cilju analize uticaja *Wavelet* porodice na kvalitet detekcije analizirana je brzina detekcije, odnosno obim kašnjenja detekcije u odnosu na stvarnu promjenu funkcije gustine vjerovatnoće signala, odnosno početak GPS *spoofing* napada.Takođe je posmatrana i vrijednost $L2$ mjere u trenutku detekcije GPS *spoofing* napada, veća vrijednost $L2$ mjere označava veću sigurnost algoritma u tačnost detekcije.

Pored analize uticaja odabira *Wavelet* porodice, analiziran je i uticaj korišćenja skalirane *Wavelet* funkcije prozora u cilju dobijanja odgovarajućih koeficijenata razvoja *Wavelet* transformacije. Rezultati su i u ovom slučaju posmatrani kroz prizmu obima kašnjenja detekcije u odnosu na stvarni početak promjene funkcije gustine vjerovatnoće signala i vrijednosti same $L2$ mjere u trenucima detekcije.

Za potrebe samog eksperimenta posmatrani su sistemi sa **14**, **57** i **118** čvorova. Generisano je po **10** signala koji simuliraju svaku od pomenutih topologija i njima je pridodat šum standardne devijacije **0.01**. Ovako generisani signali podvrgnuti su eksperimentima u kojima su korišćene *Wavelet* funkcije prozora porodica sa ortogonalnim vektorskim bazama, a rezultati eksperimenata temeljno su opisani u nastavku.

7.1.1 Rezultati eksperimenta

Daubachies Wavelet

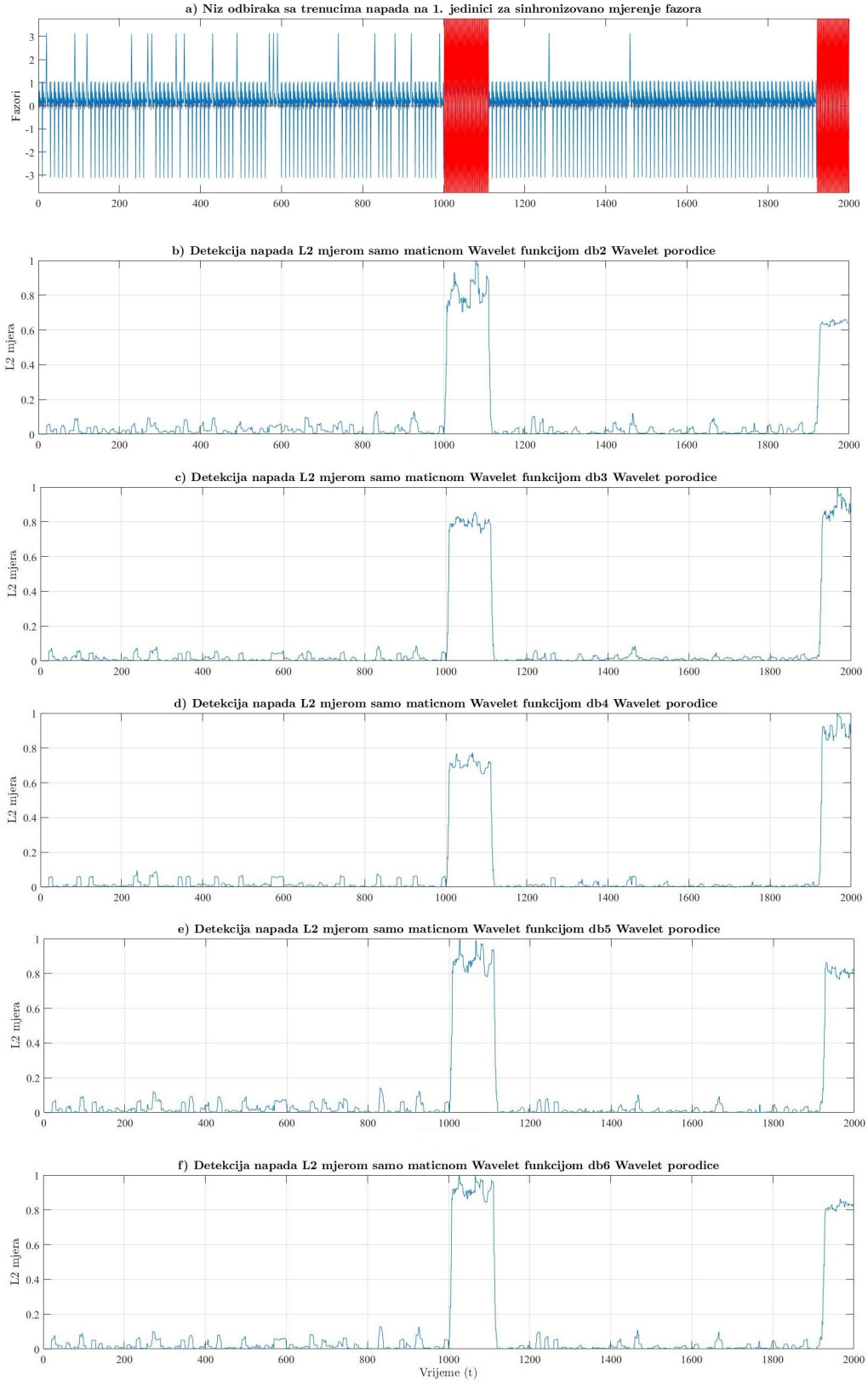
Na slikama 18 - 21 je prikazan uticaj *Daubachies Wavelet* porodice na detekciju promjene funkcije gustine vjerovatnoće signala. Na ovim slikama, na graficima označenim kao a) su prikazani odbirci originalnog fazorskog mjerenja, a crvenom bojom su obilježeni odbirci, fazori, na kojima je dodat fazni pomak, odnosno za koje se smatra da su pod GPS *spoofing* napadom. Signal koji se analizira dobijen je konkatenacijom 200 uzastopnih fazorskih mjerenja na prvoj jedinici za sinhronizovano mjerenje fazora (na slici 12 - PMU 1).

Na slikama 18 i 19 prikazana je detekcija GPS *spoofing* napada korišćenjem samo matične *Wavelet* funkcije prozora *Daubachies Wavelet* porodice sa rangom funkcije **2, 3, 4, 5, 6, 7, 8, 9** i **10**.

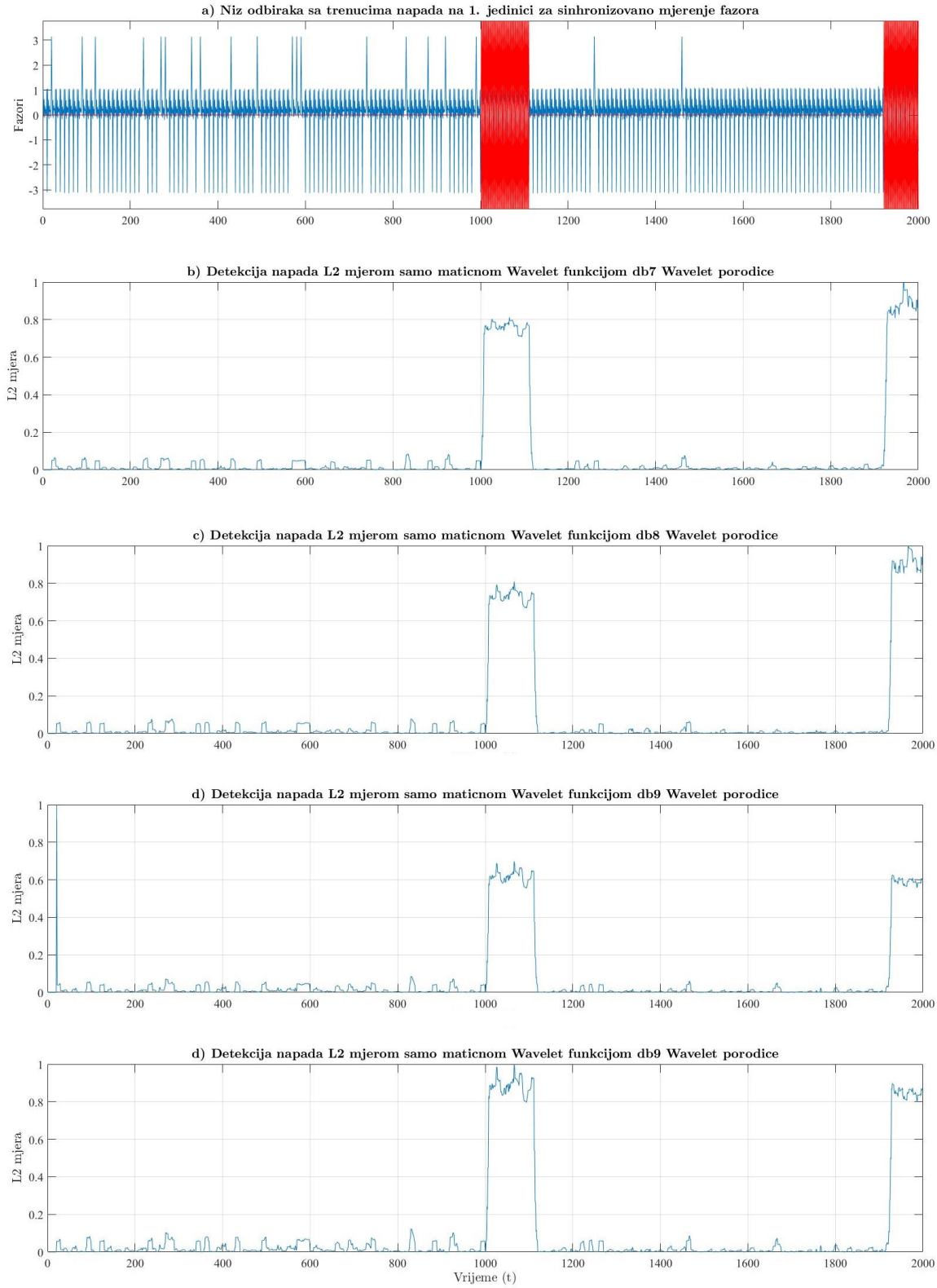
Na slici 18, na graficima b) - e) prikazane su detekcije promjene funkcije gustine vjerovatnoće signala, odnosno, GPS *spoofing* napada korišćenjem *Daubachies Wavelet* porodice i *Wavelet* funkcija prozora ranga **2, 3, 4, 5** i **6**. Na slici 19 je prikazana detekcija GPS *spoofing* napada korišćenjem *Daubachies Wavelet* porodice i to *Wavelet* funkcija ranga **7, 8, 9** i **10**.

Posmatrajući rezultate na slikama 18 i 19 može se primijetiti da prilikom promjene ranga *Wavelet* funkcije ne dolazi do značajnih promjena u kvalitetu detekcije u pogledu brzine detekcije. Dodatno, primjetno je da sa porastom ranga *Wavelet* baze vrijednosti $L2$ mjere u trenucima napada ne pokazuju sistematsko povećanje ili poboljšanje.

Dobijeni rezultati potvrđuju početnu pretpostavku da upotreba *Wavelet* funkcija višeg reda ne doprinosi značajnom poboljšanju performansi. Stoga se njihovim izbjegavanjem može postići smanjenje računske složenosti bez gubitka preciznosti.



Slika 18: Detekcija promjene funkcije gustine vjerovatnoće signala predloženim metodom korišćenjem samo matične *Wavelet* funkcije prozora *Daubachies Wavalet* porodice: b) db2, c) db3, d) db4, e) db5, f) db6



Slika 19: Detekcija promjene funkcije gustine vjerovatnoće signala predloženim metodom korišćenjem samo matične *Wavelet* funkcije prozora *Daubachies Wavalet* porodice: b) db7, c) db8, d) db9, e) db10

Na slikama 20 i 21 prikazani su slučajevi detekcije promjene funkcije gustine vjerovatnoće signala, odnosno, GPS *spoofing* napada korišćenjem i matične i skalirane *Wavelet* funkcije prozora *Daubachies Wavelet* porodice. Na graficima označenim sa a) prikazan je originalni signal i pozicije fazora kojima je dodat fazni pomak.

Na slici 20, na graficima b) - e) prikazane su detekcije promjene funkcije gustine vjerovatnoće signala korišćenjem funkcija prozora *Daubachies Wavelet* porodice, ranga **2, 3, 4, 5** i **6**, dok su na slici 21, na graficima **b) - e)** prikazane detekcije GPS *spoofing* napada korišćenjem *Daubachies Wavelet* funkcija prozora, ranga **7, 8, 9** i **10**.

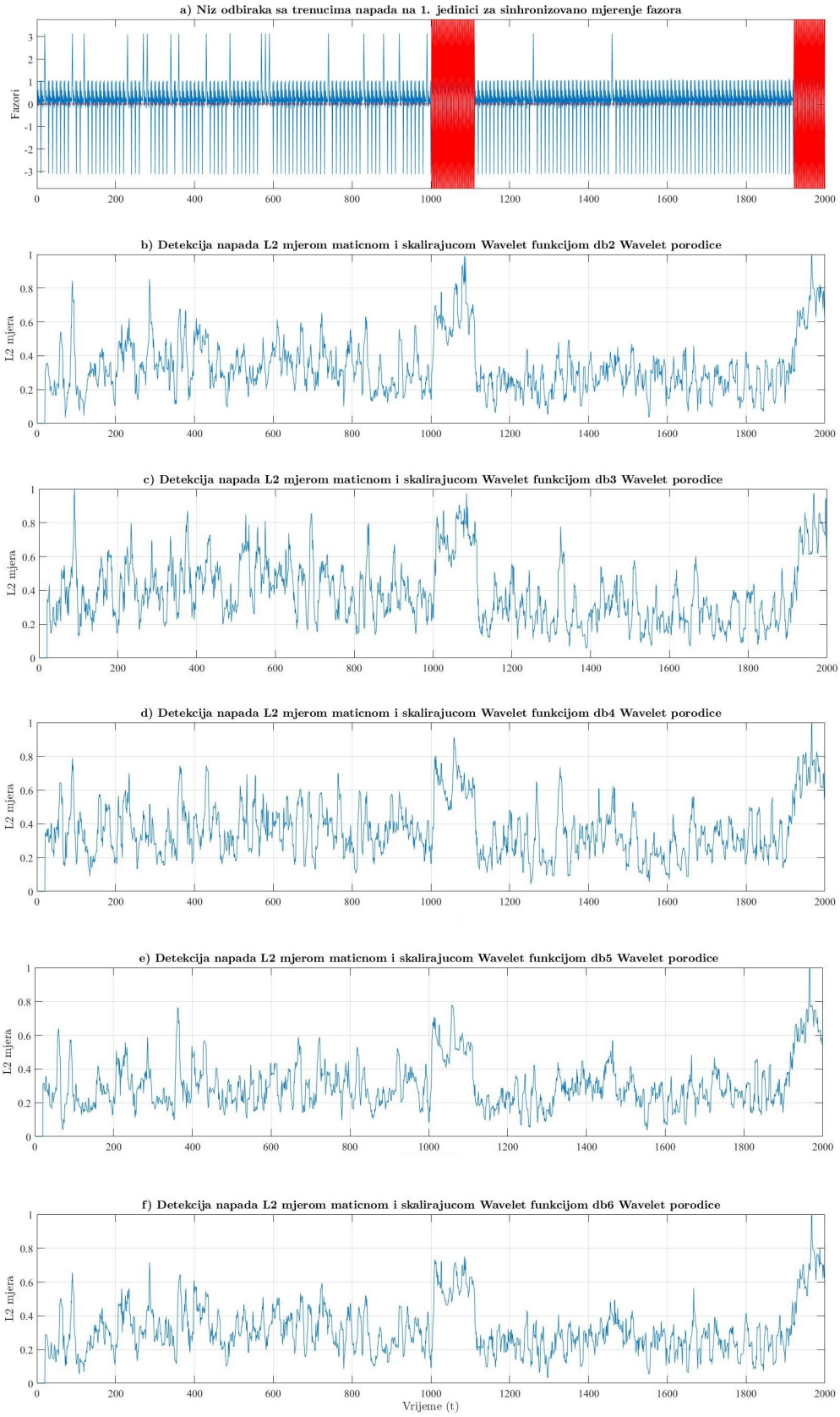
I na slici 20 i na slici 21 se može primijetiti da u slučaju korišćenja skalirane *Wavelet* funkcije prozora dolazi do pojave lažnih detekcija, kao i do velikog broja varijacija u vrijednostima signala. Iako su stvarni napadi detektovani, unošenje velikog broja varijacija može dovesti do nepotrebnih alarma.

Promjena ranga *Wavelet* funkcije ne doprinosi poboljšanju rezultata ni u slučaju brzine detekcije ni u slučaju sigurnosti algoritma. Time se može zaključiti da izbor ranga *Daubachies Wavelet* porodice ne igra važnu ulogu u detekciji promjene funkcije gustine vjerovatnoće signala, međutim, analizom detalja, pomoću skalirane *Wavelet* funkcije prozora, dolazi do degradacije rezultata.

Ova pojava se može objasniti karakteristikom koju posjeduju funkcije gustine vjerovatnoće, a to je da su glatke funkcije, što se može vidjeti i na slici 22.

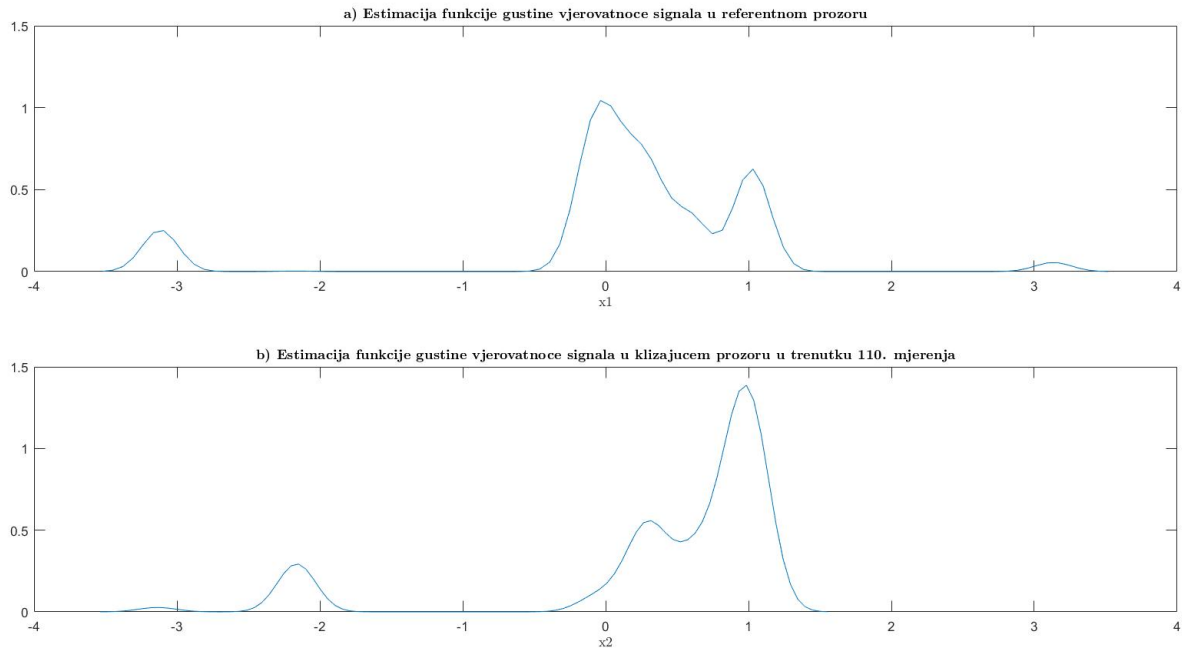
Na slici 22 je predstavljena funkcija gustine vjerovatnoće signala jezgrima (eng. *kernel density estimation*[6]) u dva vremenska trenutka: na grafiku a) je predstavljena estimacija funkcije gustine vjerovatnoće signala u referentnom prozoru, odnosno, u toku prvog mjerenja i gdje nema GPS *spoofing* napada, dok je na grafiku b) predstavljena funkcija gustine vjerovatnoće signala u klizećem prozoru u trenutku 110. mjerenja, odnosno, u toku prvog detektovanog GPS *spoofing* napada.

Može se primijetiti da postoji razlika u funkciji gustine vjerovatnoće signala, te i da su neki detalji slični. Baš zbog ovoga uvođenje skalirane *Wavelet* funkcije dovodi do degradiranja rezultata i unošenja nepotrebnog šuma u detekciju.



Slika 20: Detekcija promjene funkcije gustine vjerovatnoće signala predloženim metodom korišćenjem matične i skalirane *Wavelet* funkcije prozora *Daubachies Wavalet* porodice: b) db2, c) db3, d) db4, e) db5 i f) db6

Slika 21: Detekcija promjene funkcije gustine vjerovatnoće signala predloženim metodom korišćenjem matične i skalirane *Wavelet* funkcije prozora *Daubachies Wavalet* porodice: b) db7, c) db8, d) db9 i e) db10



Slika 22: Estimacija funkcije gustine vjerovatnoće signala u dva vremenska intervala: a) u referentnom prozoru, odnosno, u prvom mjerenju u kom nema GPS *spoofing* napada; b) u klizećem prozoru u trenutku 110. mjerenja, odnosno, u toku prvog detektovanog GPS *spoofing* napada

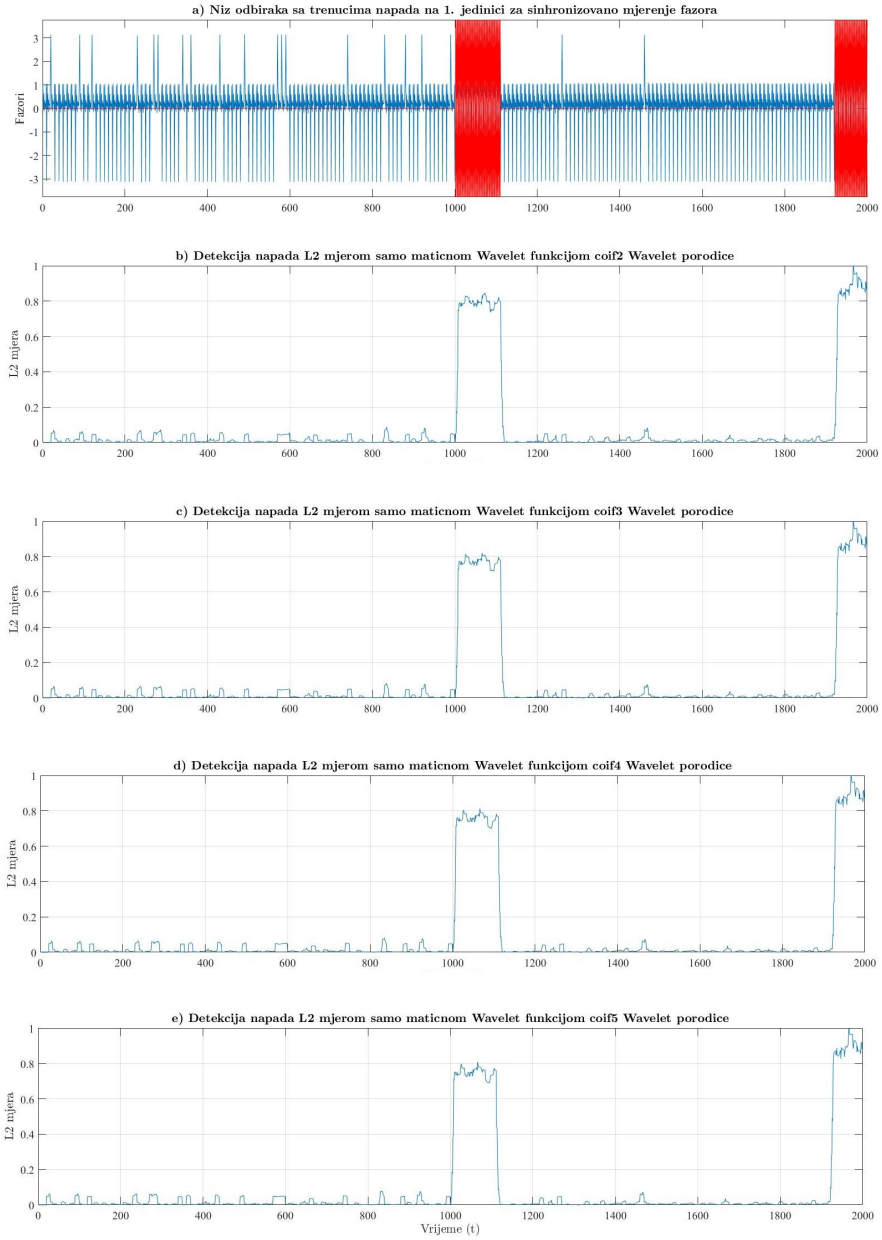
Coiflet Wavelet porodica

Na slici 23 je prikazana detekcija promjene funkcije gustine vjerovatnoće signala dobijenog konkatenacijom 200 uzastopnih mjerenja na 1. jedinici za sinhronizovano mjerenje fazora, a korišćenjem *Wavelet* funkcija prozora *Coiflet Wavelet* porodice.

Na slici 23, na grafiku a), su prikazani fazori originalnog mjerenja, dok su crvenom bojom označene pozicije fazora na kojima je dodat fazni pomak, odnosno, za koje se smatra da su pod GPS *spoofing* napadom. Na slici 23 , na graficima b) - e), su prikazane detekcije promjene funkcije gustine vjerovatnoće signala korišćenjem *Coiflet Wavelet* transformacije, ranga **2, 3, 4** i **5**, i to korišćenjem samo matične *Wavelet* funkcije prozora.

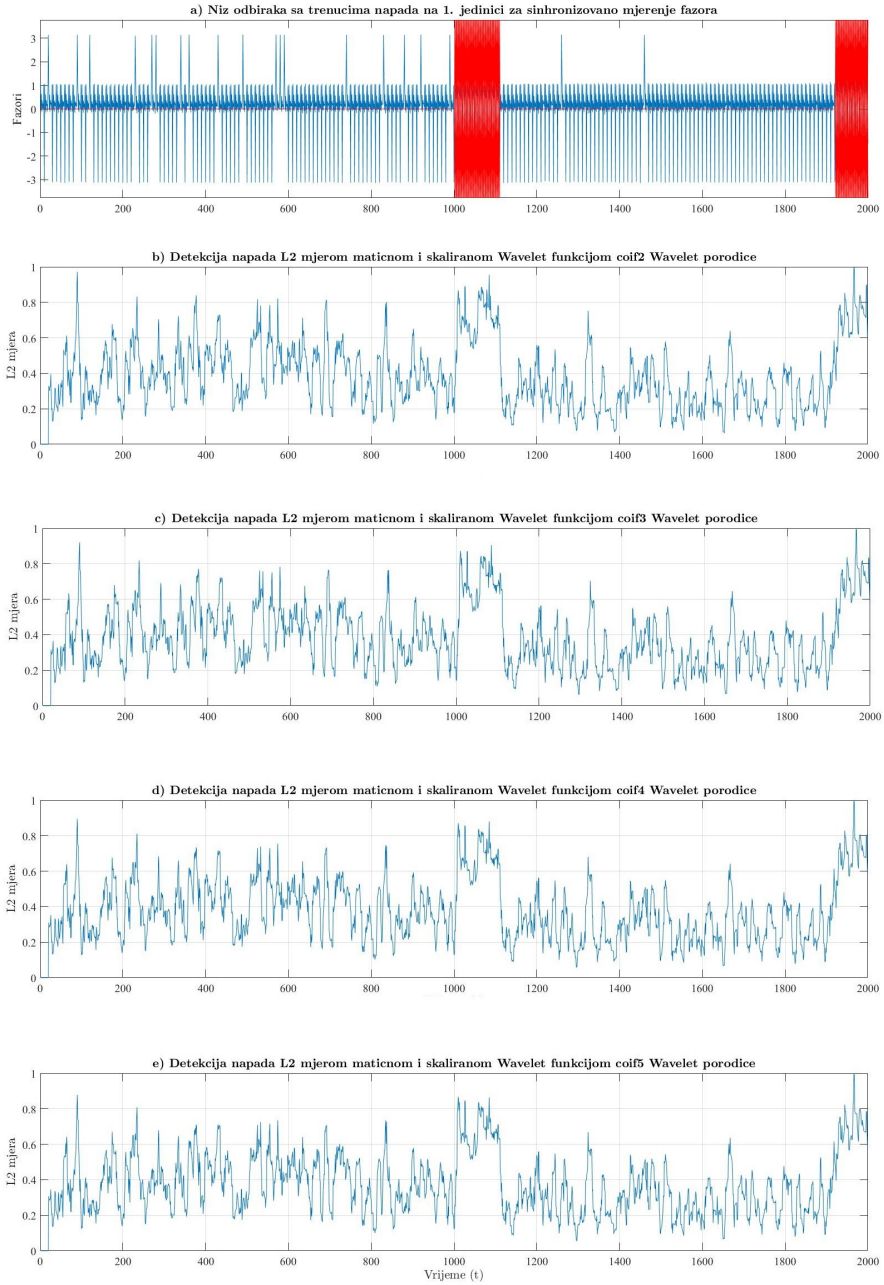
Kao i u slučaju *Daubachies Wavelet* porodice, promjena ranga *Wavelet* funkcije prozora ne doprinosi brzini detekcije GPS *spoofing* napada. Dodatno, sigurnost algoritma, odnosno vrijednost $L2$ mjere u toku napada se ne mijenja, odnosno, ne poboljšava u slučaju korišćenja *Wavelet* funkcija višeg ranga.

Prikazani rezultati još jednom pokazuju da korišćenje *Wavelet* funkcija manjeg ranga mogu obezbijediti jednaku preciznost kao i *Wavelet* funkcije višeg ranga, ali dodatno mogu smanjiti računsku kompleksnost algoritma.



Slika 23: Detekcija promjene funkcije gustine vjerovatnoće signala predloženim metodom korišćenjem samo matične *Wavelet* funkcije prozora *Coiflet Wavelet* porodice: b) coif2, c) coif3, d) coif4, e) coif5

Na slici 24, na graficima b) - e) su prikazane detekcije promjene funkcije gustine vjerovanoće signala korišćenjem funkcija prozora *Coiflet Wavelet* porodice iste konfiguracije, odnosno istih rangova kao i prethodnom slučaju. Međutim, sada je pri analizi pored matične *Wavelet* funkcije korišćena i skalirana *Wavelet* funkcija prozora.



Slika 24: Detekcija promjene funkcije gustine vjerovatnoće signala predloženim metodom korišćenjem i matične i skalirane *Wavelet* funkcije prozora *Coiflet Wavelet* porodice: b) coif2, c) coif3, d) coif4, e) coif5

U slučaju korišćenja i matične i skalirane *Wavelet* funkcije prozora pri detekciji promjene funkcije gustine vjerovatnoće signala dolazi do značajne degradacije rezultata usljed pojave lažnih detekcija, kao i pojave varijacija u vrijednostima signala, jer skalirana *Wavelet* funkcija prozora služi za analizu detalja. Sa povećanjem *Wavelet* skale skalirane *Wavelet* funkcije prozora analiziraju se sve sitniji detalji i

upravo oni dovode do nestabilnosti detekcije.

U slučaju detekcije promjene funkcije gustine vjerovatnoće signala u cilju detekcije GPS spoofing napada potrebno je analizirati nagle i izražajne promjene, stoga će fokusiranje detekcije na promjenu u detaljima signala nepotrebno degradirati rezultate.

Symlet Wavelet porodica

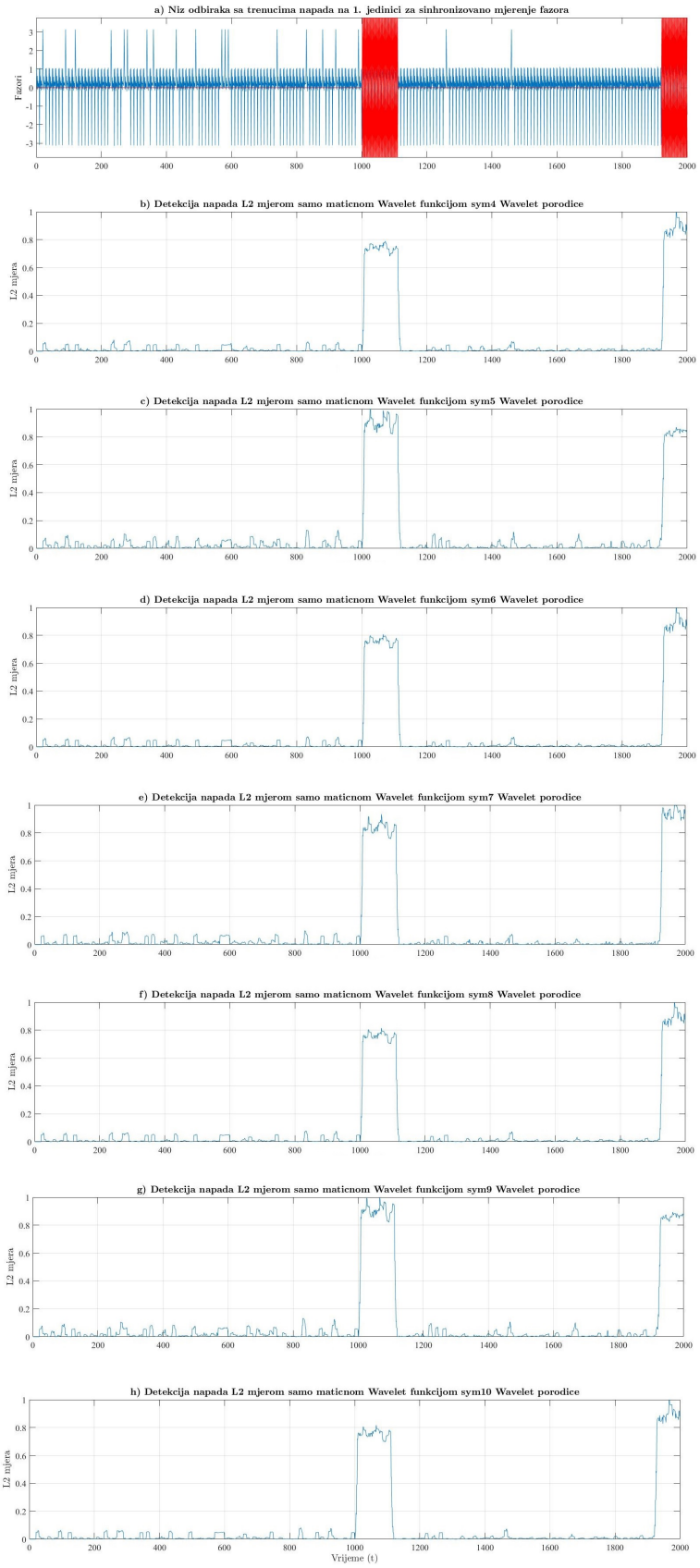
Eksperiment detekcije promjene funkcije gustine vjerovatnoće signala korišćenjem *Wavelet* funkcija prozora *Symlet Wavelet* porodice ne odstupa rezultatom od prethodno opisanih metoda. Na slikama 25 i 26 prikazani su rezultati korišćenja funkcija prozora ove *Wavelet* porodice u cilju detekcije promjene funkcije gustine vjerovatnoće signala, odnosno, GPS *spoofing* napada.

Na slici 25 su prikazani rezultati detekcije promjene funkcije gustine vjerovatnoće signala korišćenjem isključivo matične *Wavelet* funkcije prozora *Symlet Wavelet* porodice. Na slici 25, na grafiku a) prikazani su odbirci originalnog signala i pozicije odbiraka na kojima je dodat fazni pomak, označeni crvenom bojom. Na graficima b) - h) su prikazane detekcije promjene funkcije gustine vjerovatnoće signala korišćenjem *Symlet Wavelet* porodice i to ranga: **4, 5, 6, 7, 8, 9** i **10**, respektivno.

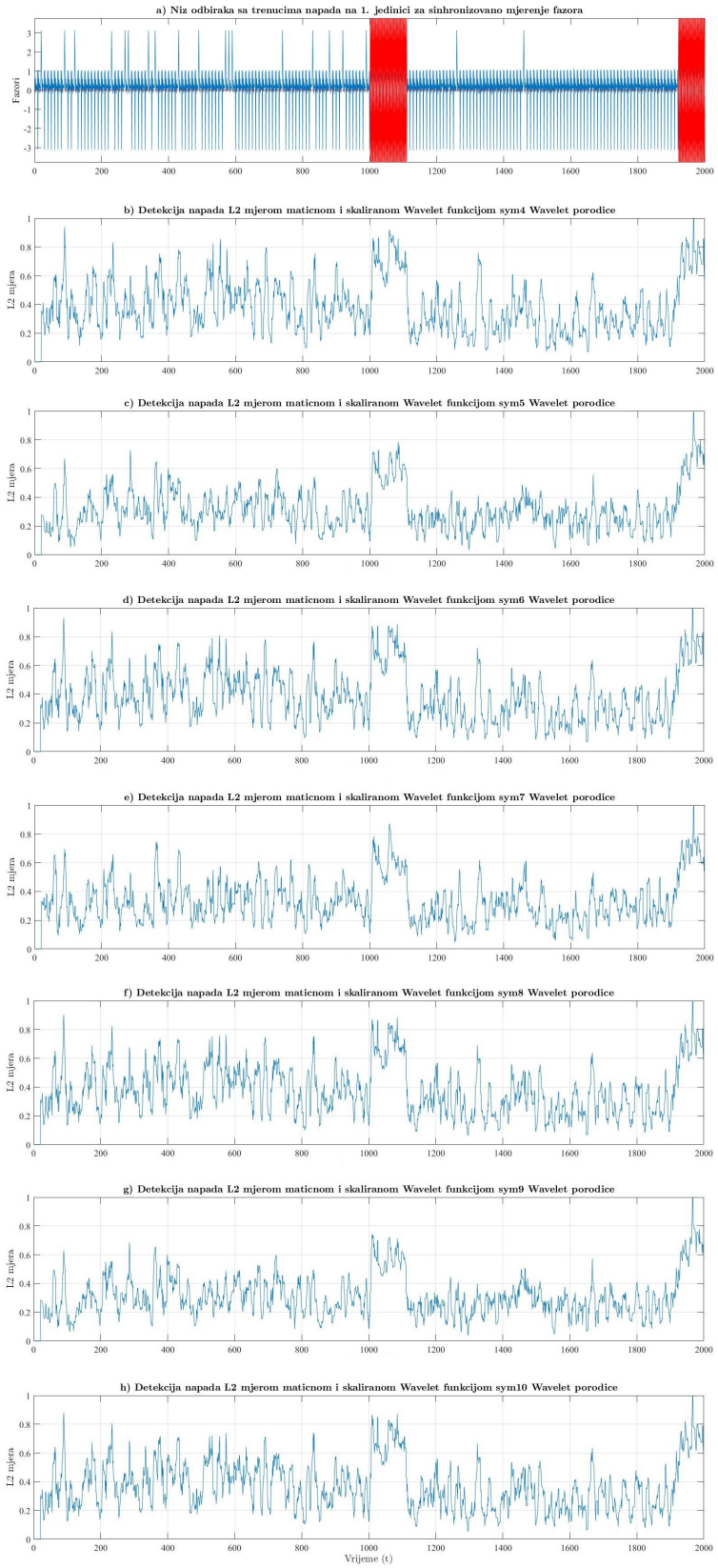
Na graficima se može primijetiti da nema značajne razlike u vrijednostima $L2$ mjere u trenucima napada sa povećavanjem ranga funkcija prozora ove porodice *Wavelet*-a. Prosječna razlika između ovih vrijednosti $L2$ mjere u trenucima detekcija ne prelazi vrijednost od **0.3**.

Na slici 26 prikazana je detekcija promjene funkcije gustine vjerovatnoće signala korišćenjem i matične i skalirane *Wavelet* funkcije prozora *Symlet Wavelet* porodice. Na grafiku a) prikazan je originalni signal sa pozicijama na kojima je dodat fazni pomak, odnosno na kojima dolazi do promjene funkcije gustine vjerovatnoće signala, označenim crvenom bojom. Na slici 26, na graficima b) - h) prikazane su detekcije promjene funkcije gustine vjerovatnoće signala korišćenjem funkcija prozora *Symlet Wavelet* porodice, ranga **4, 5, 6, 7, 8, 9** i **10**, respektivno.

Korišćenje skalirane *Wavelet* funkcije prozora u cilju detekcije GPS *spoofing* napada, ponovo daje gore rezultate u odnosu na rezultate detekcije primjenom samo matične *Wavelet* funkcije prozora. Fluktuiranje u vrijednostima signala, koje može biti izazvano bijelim šumom koji predstavlja slučajne mjerne greške, negativno utiče na povećavanje broja lažnih detekcija pri analizi detalja signala skaliranom *Wavelet* funkcijom prozora i time se zaključuje da njeno korišćenje nepotrebno degradira rezultate detekcije.



Slika 25: Detekcija promjene funkcije gustine vjerovatnoće signala predloženim metodom korišćenjem matične *Symlet Wavelet* funkcije: b) sym4, c) sym5, d) sym6, e) sym7, f) sym 8, g) sym9 i h) sym 10



Slika 26: Detekcija promjene funkcije gustine vjerovatnoće signala predloženim metodom korišćenjem matične i skalirane *Symlet Wavelet* funkcije: b) sym4, c) sym5, d) sym6, e) sym7, f) sym8, g) sym9 i h) sym10

Posmatrajući rezultate eksperimenata u kojima su korišćene *Wavelet* funkcije prozora iz sve tri *Wavelet* porodice može se zaključiti da nema značajnih promjena u detekciji prilikom promjene *Wavelet* porodice. Detekcije GPS *spoofing* napada predloženim metodom ne zavisi od promjene ranga *Wavelet* funkcije prozora, te se detekcija korišćenjem *Wavelet* funkcije nižeg ranga može obaviti jednako precizno kao i korišćenjem *Wavelet* funkcija višeg ranga, a uz manju računsku složenost.

Takođe, korišćenje skalirane *Wavelet* funkcije prozora ne daje zadovoljavajuće rezultate zato što analiza detalja unosi suvišan šum u detekciju, te ju je poželjno izbjegavati.

Prosječno vrijeme kašnjenja detekcije korišćenjem funkcija prozora iz sve tri porodice *Wavelet*-a ne prelazi polovinu dužine prozora, odnosno, broja odbiraka u jednom mjerenju. Ovo znači da će u slučaju detekcije promjene funkcije gustine vjerovatnoće signala, a u cilju detekcije GPS *spoofing* napada, detekcija biti izvršena u toku prvog seta mjerenja koja su podvrgnuta napadu.

Zaključak

Metod detekcije promjene funkcije gustine vjerovatnoće signala računanjem $L2$ mjere između koeficijenata razvoja *Wavelet* funkcije prozora u dijelu signala obuhvaćenim referentnim prozorom i dijela signala obuhvaćenim klizećim prozorom može uspješno detektovati GPS *spoofing* napade na simuliranim podacima jedinica za sinhronizovano mjerenje fazora. U odnosu na druge mjere detekcije, koje podrazumijevaju detekciju računanjem mjere maksimalne vjerovatnoće ili relativne entropije nad estimacijama funkcije gustine vjerovatnoće signala histogramom i estimiranjem parametara pretpostavljene Gausove raspodjele, pokazuje stabilnije rezultate u pogledu promjene intenziteta u slučaju stvarnih detekcija, te i manjih fluktuacija signala detekcije u periodima neizmijenjene funkcije gustine vjerovatnoće signala.

U rezultatima opisanih eksperimenata je pokazano da uspješnost detekcije i brzina detekcije promjene funkcije gustine vjerovatnoće signala neće zavisiti od izbora *Wavelet* porodice. Takođe, pokazano je da izbor *Wavelet* funkcija većeg ranga neće dovesti do izraženije promjene $L2$ mjere i doprinijeti bržem izvršavanju algoritma, te se uz jednaku preciznost mogu koristiti *Wavelet* funkcije nižeg ranga. Korišćenje skalirane *Wavelet* funkcije prozora, bilo koje *Wavelet* porodice, dovodi do fluktuacija u vrijednosti signala detekcije i dovodi do pojave lažnih detekcija, a ujedno i usložnjava algoritam i povećava vrijeme izvršavanja, te se preporučuje njeno izbjegavanje.

Ograničenje ovog istraživanja predstavlja korišćenje sintetičkog seta podataka u eksperimentima i ostavlja prostor za unaprijeđivanjem u primjeni na realnom *dataset*-u. Dalja istraživanja primjene metoda bi podrazumijevala analizu ostalih faktora koji mogu uticati na detekciju GPS *spoofing* napada, a koja su očekivana u realnim uslovima, kao što su prekidi, preklapanja i preusmjeravanja napona, odnosno struja, tokom rada mreže i drugi faktori koji se tiču topologije samog elektroenergetskog sistema. Takođe, mogao bi se analizirati slučaj pojave GPS *spoofing* napada u kombinaciji sa nekim drugim sajber napadom ili uticaj prirodnih faktora na rad mreže kao što su uticaj magnetnog polja u blizini jedinica za sinhronizovano mjerenje fazora. Dodatno, predmet dalje analize može biti i primjena metoda detekcije promjene funkcije gustine vjerovatnoće signala na detekciju drugih sajber napada u energetici, ali i u drugim privrednim oblastima.

Literatura

[1] Charles Truong, Laurent Oudre, and Nicolas Vayatis. Selective review of offline change point detection methods. *Signal Processing*, 167:107299, 2020.

[2] In Jae Myung. Tutorial on maximum likelihood estimation. *Journal of mathematical Psychology*, 47(1):90–100, 2003.

[3] Michael R. Berthold and David J. Hand. *Intelligent Data Analysis: An Introduction*. Springer, 2007.

[4] John R Hershey and Peder A Olsen. Approximating the kullback leibler divergence between gaussian mixture models. In *2007 IEEE International Conference on Acoustics, Speech and Signal Processing-ICASSP'07*, volume 4, pages IV–317. IEEE, 2007.

[5] Wei Gao, Haizhong Yang, and Lu Yang. Change points detection and parameter estimation for multivariate time series. *Soft Computing*, 24(9):6395–6407, 2020.

[6] Hoseung Song and Hao Chen. Practical and powerful kernel-based change-point detection. *IEEE Transactions on Signal Processing*, 72:5174–5186, 2024.

[7] Nenad Mijatovic, Rana Haber, Mark Moyou, Anthony O Smith, and Adrian M Peter. Change detection for streaming data using wavelet-based least squares density–difference. In *International Conference on Time Series and Forecasting*, pages 99–116. Springer, 2018.

[8] Edgar S García-Treviño and Javier A Barria. Online wavelet-based density estimation for non-stationary streaming data. *Computational statistics & data analysis*, 56(2):327–344, 2012.

[9] Der-Yeuan Yu, Aanjhan Ranganathan, Thomas Locher, Srdjan Capkun, and David Basin. Short paper: Detection of gps spoofing attacks in power grids. In *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*, pages 99–104, 2014.

[10] Sriramya Bhamidipati, Kyeong Jin Kim, Hongbo Sun, and Philip V Orlik. Gps spoofing detection and mitigation in pmus using distributed multiple directional antennas. In *ICC 2019-2019 IEEE International Conference on Communications (ICC)*, pages 1–7. IEEE, 2019.

[11] Mohammad Sabouri, Sara Siamak, Maryam Dehghani, Mohsen Mohammadi, and Mohammad Hassan Asemani. Intelligent gps spoofing attack detection in power grid. In *2021 11th Smart Grid Conference (SGC)*, pages 1–6. IEEE, 2021.

[12] Fayha Almutairy, Lazar Scekic, Mustafa Matar, Ramadan Elmoudi, and Safwan Wshah. Detection and mitigation of gps spoofing attacks on phasor measurement units using deep learning. *International Journal of Electrical Power & Energy Systems*, 151:109160, 2023.

[13] Ying Zhang, Jianhui Wang, and Jianzhe Liu. Attack identification and correction for pmu gps spoofing in unbalanced distribution systems. *IEEE transactions on smart grid*, 11(1):762–773, 2019.

[14] Sara Siamak, Maryam Dehghani, and Mohsen Mohammadi. Dynamic gps spoofing attack detection, localization, and measurement correction exploiting pmu and scada. *IEEE Systems Journal*, 15(2):2531–2540, 2020.

[15] Xiao Wei, Muhammad Naveed Aman, and Biplab Sikdar. Light-weight gps spoofing detection for synchrophasors in smart grids. In *2020 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES)*, pages 1–4. IEEE, 2020.

[16] Ying Zhang, Jianhui Wang, and Jianzhe Liu. Attack identification and correction for pmu gps spoofing in unbalanced distribution systems. *IEEE transactions on smart grid*, 11(1):762–773, 2019.

[17] Der-Yeuan Yu, Aanjhan Ranganathan, Thomas Locher, Srdjan Capkun, and David Basin. Short paper: Detection of gps spoofing attacks in power grids. In *Proceedings of the 2014 ACM conference on Security and privacy in wireless & mobile networks*, pages 99–104, 2014.

[18] Xiao Wei, Muhammad Naveed Aman, and Biplab Sikdar. Light-weight gps spoofing detection for synchrophasors in smart grids. In *2020 IEEE International Conference on Power Electronics, Drives and Energy Systems (PEDES)*, pages 1–4. IEEE, 2020.

[19] Fayha Almutairy, Lazar Scekic, Mustafa Matar, Ramadan Elmoudi, and Safwan Wshah. Detection and mitigation of gps spoofing attacks on phasor measurement units using deep learning. *International Journal of Electrical Power & Energy Systems*, 151:109160, 2023.

[20] Ljubisa Stankovic. *Digital Signal Processing*. CreateSpace Independent Publishing Platform, 11 2015.

[21] Md. Wajed Ali, Tanvir Ahmmed, Md Al Emran, Dipon Roy, Kawsar Ahmed Refat, and Robiul Khan. Driver fatigue detection using cwt-extracted features and a deep learning approach (cnnlstm). In *2024 IEEE International Conference on Biomedical Engineering, Computer and Information Technology for Health (BECITHCON)*, pages 77–82, 2024.

[22] Ivo B Gonçalves, Ana Leiria, and MMM Moura. Stft or cwt for the detection of doppler ultrasound embolic signals. *International journal for numerical methods in biomedical engineering*, 29(9):964–976, 2013.

[23] Ghassen Smaoui, Alex Young, and Mohamed Abid. Single scale cwt algorithm for ecg beat detection for a portable monitoring system. *Journal of Medical and Biological Engineering*, 37:132–139, 2017.

[24] Emiel Por, Maaike van Kooten, and Vanja Sarkovic. Nyquist–shannon sampling theorem. *Leiden University*, 1(1):1–2, 2019.

[25] Clemens Valens. A really friendly guide to wavelets. 1999.

[26] Piotr Porwik and Agnieszka Lisowska. The haar-wavelet transform in digital image processing: its status and achievements. *Machine graphics and vision*, 13(1/2):79–98, 2004.

[27] Cédric Vonesch, Thierry Blu, and Michael Unser. Generalized daubechies wavelet families. *IEEE transactions on signal processing*, 55(9):4415–4429, 2007.

[28] Siripurapu Sridhar, P Rajesh Kumar, and KV Ramanaiah. Wavelet transform techniques for image compression-an evaluation. *International journal of image, graphics and signal processing*, 6(2):54, 2014.

[29] N.N. Cencov. Estimation of an unknown distribution density from observations. *Soviet Mathematics*, 3:1559–1562, 1962.

[30] Rangarajan A. Peter AM. Maximum likelihood wavelet density estimation with applications to image and shape matching. *IEEE Trans Image Process*, 17(4):458–68, 04 2008.

[31] Samaneh Aminikhanghahi and Diane J Cook. A survey of methods for time series change point detection. *Knowledge and information systems*, 51(2):339–367, 2017.

[32] Hans-Georg Müller and Alexander Petersen. Density estimation including examples. *Wiley StatsRef: Statistics Reference Online*, pages 1–12, 2016.

[33] Sung-Hyuk Cha. Comprehensive survey on distance/similarity measures between probability density functions. *City*, 1(2):1, 2007.

[34] Elspec Ltd. G5 phasor measurement unit. `https://www.elspec-ltd.com/metering-protection/g5-phasor-measurement-unit/`, 2024. Pristupljeno: 14. novembar 2024.

[35] Grazia Barchi et al. Algorithms and performance analysis for synchrophasor and grid state estimation. 2015.

[36] Janne Seppänen et al. Methods for monitoring electromechanical oscillations in power systems. 2017.

[37] IEEE/IEC International Standard - Measuring relays and protection equipment - Part 118-1: Synchrophasor for power systems - Measurements, 2018, IEC/IEEE 60255-118-1:2018, 1-78.

[38] Wenpeng Yu, Wenxuan Yao, Xianda Deng, Yinfeng Zhao, and Yilu Liu. Timestamp shift detection for synchrophasor data based on similarity analysis between relative phase angle and frequency. *IEEE Transactions on Power Delivery*, 35(3):1588–1591, 2019.

[39] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srdjan Capkun. On the requirements for successful gps spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*, pages 75–86, 2011.

[40] Peng Yang, Zhao Tan, Ami Wiesel, and Arye Nehorai. Power system state estimation using pmus with imperfect synchronization. *IEEE Transactions on power Systems*, 28(4):4162–4172, 2013.

[41] Ray D. Zimmerman, Carlos E. Murillo-Sánchez, and Robert J. Thomas. *MATPOWER Case14 Data*. MATPOWER, Version 7.1, 2016. Available at: `https://matpower.org`.

[42] Dong Wei. *Coiflet-type wavelets: theory, design, and applications*. The University of Texas at Austin, 1998.

[43] E.G.T. Swee and S. Elangovan. Applications of symlets for denoising and load forecasting. In *Proceedings of the IEEE Signal Processing Workshop on Higher-Order Statistics. SPW-HOS '99*, pages 165–169, 1999.

Izjava o istovjetnosti štampane i elektronske verzije master rada

Ime i prezime autora Anja Brtan
Broj indeksa/upisa 7/21
Studijski program Računari
Naslov rada
Detekcija promjene funkcije gustine vjerovatnoće signala sa primjenom na identifikaciju GPS *spoofing* napada na uređaje za sinhronizovano mjerenje fazora
Mentor Prof. dr Vesna Popović – Bugarin

Potpisani/a Anja Brtan

Izjavljujem

da je štampana verzija mog master rada istovjetna elektronskoj verziji koju sam predao/la za objavljivanje u Digitalni arhiv Univerziteta Crne Gore.

Istovremeno izjavljujem da dozvoljavam objavljivanje mojih ličnih podataka u vezi sa dobijanjem akademskog naziva master nauka, kao što su ime i prezime, godina i mjesto rođenja, naslov master rada i datum odbrane rada.

U Podgorici, 25.11.2025. godine

Potpis magistranda

Anja Brtan

IZJAVA O KORIŠĆENJU

Ovlašćujem Univerzitetsku biblioteku da u Digitalnom arhivu Univerziteta Crne Gore pohrani moj master rad pod nazivom:

" Detekcija promjene funkcije gustine vjerovatnoće signala sa primjenom na identifikaciju GPS *spoofing* napada na uređaje za sinhronizovano mjerenje fazora "

koji je moje autorsko djelo.

Master rad sa svim prilozima predao/la sam u elektronskom formatu pogodnom za trajno arhiviranje.

Moj master rad pohranjen u Digitalnom arhivu Univerziteta Crne Gore mogu da koriste svi koji poštuju odredbe sadržane u odabranom tipu licence Kreativne zajednice (*Creative Commons*) za koju sam se odlučio/la.

1. Autorstvo
2. Autorstvo – nekomercijalno
3. Autorstvo – nekomercijalno – bez prerade
4. Autorstvo – nekomercijalno – dijeliti pod istim uslovima
5. Autorstvo – bez prerade
6. Autorstvo – dijeliti pod istim uslovima

(Molimo da zaokružite samo jednu od šest ponuđenih licenci, kratak opis licenci dat je na poleđini lista).

U Podgorici, 25.11.2025. godine

Potpis magistranda

Anja Bretan

1. Autorstvo - Dozvoljavate umnožavanje, distribuciju i javno saopštavanje djela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence, čak i u komercijalne svrhe. Ovo je najslobodnija od svih licenci.

2. Autorstvo - nekomercijalno. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje djela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu djela.

3. Autorstvo - nekomercijalno - bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje djela, bez promjena, preoblikovanja ili upotrebe djela u svom djelu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu djela. U odnosu na sve ostale licence, ovom licencom se ograničava najveći obim prava korišćenja djela.

4. Autorstvo - nekomercijalno - dijeliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje djela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca ne dozvoljava komercijalnu upotrebu djela i prerade.

5. Autorstvo - bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje djela, bez promjena, preoblikovanja ili upotrebe djela u svom djelu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca dozvoljava komercijalnu upotrebu djela.

Autorstvo - dijeliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje djela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca dozvoljava komercijalnu upotrebu djela i prerada. Slična je softverskim licencama, odnosno licencama otvorenog koda