POLITECHNIKA GDAŃSKA
WYDZIAŁ ELEKTRONIKI, TELEKOMUNIKACJI I INFORMATYKI

Imię i nazwisko autora rozprawy: Jarosław Magiera
Dyscyplina naukowa: Telekomunikacja

ROZPRAWA DOKTORSKA

Tytuł rozprawy w języku polskim: Analiza i badania systemu antyspoofingowego GPS

Tytuł rozprawy w języku angielskim: Analysis and research on GPS antispoofing system

Promotor *podpis*	Drugi promotor *podpis*
prof. dr hab. inż. Ryszard J. Katulski	
Promotor pomocniczy *podpis*	Kopromotor *podpis*

Gdańsk, rok 2015

mojemu synowi - Krzysztofowi

Pragnę podziękować wszystkim pracownikom
Katedry Systemów i Sieci Radiokomunikacyjnych
Politechniki Gdańskiej, którzy okazali mi wsparcie
przy pracy nad niniejszą rozprawą.

Spis treści

Wprowadzenie

Przedmiotem niniejszej rozprawy doktorskiej są analizy i badania, zmierzające do rozwiązania problemu naukowego, jakim jest wypracowanie efektywnych metod przeciwdziałania zjawisku określanemu mianem spoofingu GPS. Pod pojęciem spoofing (z ang. "podszywanie się") rozumie się, w tym przypadku, transmisję fałszywych sygnałów systemu nawigacji satelitarnej GPS (Global Positioning System), mającą na celu doprowadzenie do wyznaczenia, przez odbiornik tych sygnałów, nieprawidłowych informacji o jego położeniu, prędkości i aktualnym czasie. Nadajnik fałszywych sygnałów, nazywany spooferem, "podszywa się" pod konstelację satelitów systemu GPS.

Motywacją do podjęcia analiz i badań opisywanych w tej rozprawie, był, zrealizowany w Katedrze Systemów i Sieci Radiokomunikacyjnych Politechniki Gdańskiej, projekt badawczo-rozwojowy, dotyczący technologii zakłócania transmisji sygnałów z bezpośrednio rozproszonym widmem DS-CDMA [43]. W ramach tego projektu, którego głównym wykonawcą był autor niniejszej rozprawy, analizowano wpływ oddziaływania różnego rodzaju celowych interferencji radiowych na poprawność pracy odbiorników globalnych systemów nawigacji satelitarnej GNSS, w tym systemu GPS. Prowadzone badania dotyczyły zarówno możliwości zagłuszania sygnałów nawigacji satelitarnej przy użyciu wąsko- i szerokopasmowych sygnałów zakłócających, jak również podatności odbiorników GPS na spoofing. Uzyskane wyniki wskazały jednoznacznie, że realizacja spoofingu w systemie GPS jest możliwa, a dostępne na rynku odbiorniki nawigacyjne tego systemu nie są należycie zabezpieczone przed tego rodzaju atakami.

W związku z powyższym, postanowiono określić możliwości implementacji metod ochro-

ny przed spoofingiem. W pierwszej kolejności przeprowadzono przegląd literatury przedmiotu, w celu usystematyzowania stanu wiedzy na temat istniejących sposobów przeciwdziałania spoofingowi. Dokonano oceny rozwiązań proponowanych w literaturze, pod kątem ich efektywności i złożoności implementacji. Zidentyfikowano również zasadnicze ograniczenia, wiążące się z zastosowaniem konkretnych metod.

Po dokonaniu oceny istniejących rozwiązań, opracowano autorską metodę wykrywania spoofingu GPS, w której detekcja jest oparta o wartości parametrów związanych z charakterystyką przestrzenną odbieranych sygnałów. Ta metoda jest zasadniczym elementem koncepcji systemu antyspoofingowego, będącego przedmiotem analiz i badań podjętych przez doktoranta, i stanowi punkt wyjścia do sformułowania tezy niniejszej rozprawy. Zgodnie z opracowaną koncepcją, system antyspoofingowy umożliwia nie tylko wykrycie spoofingu, ale również jego eliminację, rozumianą jako zminimalizowanie jego wpływu na pracę odbiornika GPS. Jako metodę eliminacji zastosowano adaptacyjne kształtowanie charakterystyki odbiorczej szyku antenowego, tak aby stłumić na wejściu odbiornika sygnały nadawane przez spoofer. Proces eliminacji spoofingu bazuje na wartościach parametrów wyznaczonych podczas etapu jego wykrywania.

Mając na uwadze przeprowadzoną analizę problemu naukowego i założony sposób jego rozwiązania, podjęto wykonanie badań, mających na celu wykazanie prawdziwości stwierdzeń zawartych w tezie rozprawy.

W pierwszej kolejności przystąpiono do realizacji badań symulacyjnych. Ich głównym celem było potwierdzenie zasadności stosowania przyjętych metod detekcji i eliminacji spoofingu. Badania te stanowią oryginalny dorobek autora rozprawy. Brak jest publikacji dotyczących podobnych analiz innych metod, w związku z czym było konieczne określenie nowego zbioru uniwersalnych parametrów jakościowych, które umożliwiają dokonanie jednoznacznej oceny funkcjonowania rozwiązań antyspoofingowych.

Wyniki symulacji ukazują obraz działania systemu w warunkach modelowych, które nie uwzględniają wszystkich czynników, mających wpływ na jego efektywność. Zbadanie jakości pracy systemu antspoofingowego w warunkach rzeczywistych wymagało przeprowadzenia weryfikacji pomiarowej. W tym celu zbudowano prototyp tego systemu i, z jego użyciem, wykonano szereg

pomiarów w różnych wariantach transmisji fałszywych i prawdziwych sygnałów GPS. Wyniki tych pomiarów stanowią podstawę do ostatecznej oceny analizowanego rozwiązania i jednocześnie wskazują kierunki dalszych prac.

Niniejszą rozprawę podzielono na sześć rozdziałów. Pierwszy z nich ma charakter wprowadzający i stanowi charakterystykę systemu GPS w kontekście jego niezawodności i bezpieczeństwa. Szczególny nacisk został położony na kwestię odporności odbiorników nawigacyjnych na ataki typu spoofing. W rozdziale pierwszym zdefiniowano również cel i tezę rozprawy.

Rozdział drugi stanowi przegląd metod wykrywania i detekcji spoofingu, ze szczególnym uwzględnieniem metod bazujących na przestrzennym przetwarzaniu sygnałów nadawanych przez spoofer. Dokonano analizy porównawczej metod wykrywania spoofingu pod kątem ich skuteczności i złożoności ich implementacji.

Począwszy od rozdziału trzeciego, rozprawa stanowi prezentację oryginalnego dorobku doktoranta. W tym rozdziale zaproponowano koncepcję nowego, kompleksowego rozwiązania antyspoofingowego. Zawarto tu m.in. informacje dotyczące poszczególnych etapów przetwarzania sygnałów GPS w proponowanym systemie, w odniesieniu do algorytmów stosowanych w tradycyjnych odbiornikach GPS.

Rozdział czwarty poświęcono przedstawieniu metodologii i wyników badań symulacyjnych przeprowadzonych przez autora rozprawy. Rezultaty tych badań umożliwiają dokonanie wstępnej oceny efektywności przyjętych metod detekcji i eliminacji spoofingu GPS.

W rozdziale piątym opisano sposób realizacji prototypu systemu antyspoofingowego. Prototyp ten stanowi praktyczną implementację koncepcji opisanej w rozdziale 3. Intencją jego wykonania było przetestowanie funkcjonowania zaproponowanych rozwiązań w warunkach rzeczywistych.

Ostatni, szósty rozdział zawiera opis i wyniki badań pomiarowych, wykonanych z użyciem stanowiska badawczego, którego głównym elementem jest wspomniany prototyp. Badania te przeprowadzono aby: zweryfikować poprawność wyników symulacji, zidentyfikować ewentualne rozbieżności pomiędzy wynikami symulacji i pomiarów, ostatecznie ocenić efektywność przyjętych rozwiązań, jak również ustalić kierunki dalszych badań i rozwoju systemu.

Rozdział 1

Spoofing w systemie GPS

W niniejszym rozdziale omówiono zagadnienie bezpieczeństwa standardowej (tzw. cywilnej) usługi określania położenia, oferowanej przez system nawigacji satelitarnej GPS. Podatność tej usługi na różnego rodzaju ataki elektroniczne stała się motywacją do przeprowadzenia analiz i badań, które zostały opisane w rozprawie.

Pierwsza część rozdziału jest poświęcona parametrom sygnałów GPS, decydującym o możliwości celowego zakłócenia lub modyfikacji tych sygnałów. Następnie jest zdefiniowane pojęcie spoofingu, jako ataku powodującego wyznaczanie niepoprawnych informacji nawigacyjnych przez odbiornik GPS. W ostatniej części przedstawiono cel realizowanych badań i zdefiniowano tezę rozprawy doktorskiej.

1.1 System nawigacyjny GPS i jego niezawodność

Poniżej dokonano krótkiej charakterystyki systemu GPS, ze szczególnym uwzględnieniem parametrów sygnałów przesyłanych w interfejsie radiowym satelita-odbiornik. Przeanalizowano również czynniki, które mogą negatywnie wpływać na dostępność usługi lokalizacyjnej, tzn. utrudniać wyznaczenie poprawnej pozycji, prędkości i czasu przez odbiornik GPS. Jednym z takich czynników jest obecność spoofingu, którego metody wykrywania i eliminacji stanowią obiekt analiz przeprowadzonych w tej rozprawie.

1.1.1 Charakterystyka ogólna systemu GPS

System GPS-NAVSTAR (ang. Global Positioning System - NAVigation System using Timing and Ranging) jest zarządzany i nadzorowany przez Departament Obrony Stanów Zjednoczonych. W porównaniu z innymi systemami nawigacji satelitarnej GNSS, takimi jak rosyjski GLONASS, chiński Beidou czy europejski Galileo, wyróżnia się on najdłuższym czasem działania w pełnej zdolności operacyjnej, jak również największą liczbą użytkowanych odbiorników przeznaczonych do zastosowań cywilnych.

Ustalenie położenia odbiornika GNSS w przestrzeni trójwymiarowej jest możliwe w dowolnym miejscu, w którym jest możliwy poprawny odbiór co najmniej czterech sygnałów nawigacyjnych z satelitów, krążących po orbitach okołoziemskich.

Systemy GNSS składają się z trzech segmentów: naziemnego, kosmicznego i użytkownika. Segment naziemny systemu GPS stanowią stacje monitorowania i kontroli satelitów, rozmieszczone na szerokościach geograficznych bliskich równikowi i rozłożone możliwie równomiernie na różnych długościach geograficznych. Ich głównymi zadaniami są obserwacja toru ruchu satelitów i nadzór ich stanu technicznego oraz aktualizacja danych nawigacyjnych (tzw. depesz), które są następnie nadawane przez satelity.

Segment kosmiczny tworzy konstelacja trzydziestu dwóch satelitów, krążących po średnich orbitach okołoziemskich, na wysokości ponad 20 tysięcy kilometrów. Satelity systemu GPS nadają dwa rodzaje sygnałów: cywilne, których odbiór jest możliwy przez wszystkich użytkowników oraz militarne, które są zaszyfrowane i dostępne jedynie dla armii USA oraz innych tzw. użytkowników autoryzowanych. Usługa wyznaczania położenia w wariancie cywilnym jest określana mianem standardowej usługi pozycjonowania SPS. Odbiór sygnałów wojskowych umożliwia uzyskanie większej dokładności, dlatego w tym przypadku mówi się o precyzyjnej usłudze pozycjonowania PPS. Sygnały PPS są nadawane przez wszystkie satelity GPS na dwóch częstotliwościach: L1 = 1575,42 MHz oraz L2 = 1227,6 MHz, natomiast sygnały SPS jedynie na częstotliwości L1 [34].

Segment użytkownika obejmuje wszystkie rodzaje odbiorników GPS, począwszy od tzw. smartfonów i urządzeń nawigacji samochodowej, skończywszy na zaawansowanych odbiornikach

służących np. do pomiarów geodezyjnych czy nawigacji lotniczej lub kosmicznej. Z punktu widzenia niniejszej pracy najbardziej istotny jest interfejs pomiędzy segmentem kosmicznym a segmentem użytkownika, gdyż właśnie w tym miejscu występują czynniki mające bezpośredni wpływ na dostępność usługi określania położenia.

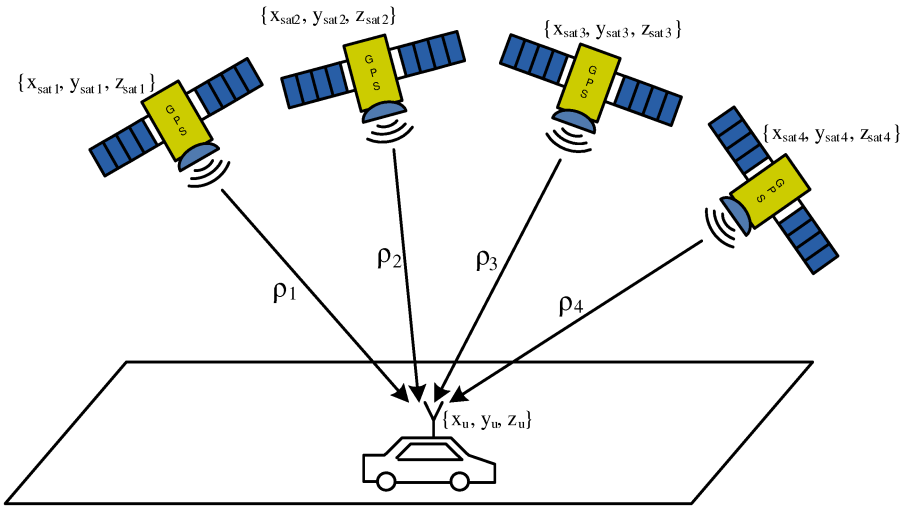
W systemie GPS, podobnie jak w innych systemach GNSS, do określenia pozycji stosowana jest metoda ToA, bazująca na pomiarze czasu propagacji sygnału od stacji referencyjnej (satelity) do odbiornika. Czas ten jest, po uwzględnieniu odpowiednich korekt, proporcjonalny do odległości pomiędzy anteną nadawczą satelity a anteną odbiornika. Lokalizacja anteny odbiornika w trzech wymiarach jest realizowana w oparciu o pomiar czasu od co najmniej czterech satelitów GPS. Zmierzone czasy umożliwiają rozwiązanie układu równań (1.1) z czterema niewiadomymi, z których trzy stanowią współrzędne pozycji odbiornika x_u, y_u, z_u, a czwartą przesunięcie t_u taktu zegara odbiornika względem zegara na pokładzie satelity. N_{sat} jest liczbą satelitów, których sygnały są odbierane w danej chwili, c jest prędkością światła w próżni, x_{sat_n}, y_{sat_n}, z_{sat_n} to współrzędne n-tego widzianego satelity, natomiastρ_i to tzw. pseudoodległość odbiornika od tego satelity, czyli estymata odległości wyznaczona na podstawie czasu propagacji sygnału.

$$\begin{cases} \rho_1 = \sqrt{(x_{s_1} - x_u)^2 + (y_{s_1} - y_u)^2 + (z_{s_1} - z_u)^2} + ct_u \\ \rho_2 = \sqrt{(x_{s_2} - x_u)^2 + (y_{s_2} - y_u)^2 + (z_{s_2} - z_u)^2} + ct_u \\ \dots \\ \rho_{N_{sat}} = \sqrt{(x_{s_{N_{sat}}} - x_u)^2 + (y_{s_{N_{sat}}} - y_u)^2 + (z_{s_{N_{sat}}} - z_u)^2} + ct_u \end{cases} \tag{1.1}$$

Można więc stwierdzić, że do wyznaczenia położenia anteny odbiorczej, odbiornik musi dysponować następującymi informacjami:

- aktualnym położeniem satelitów, których sygnały są odbierane oraz
- pseudoodległościami od tych satelitów.

Bieżące położenie każdego z satelitów jest ustalane na podstawie parametrów orbitalnych i aktualnego czasu systemowego, przesyłanych w depeszach nawigacyjnych. Z kolei czasy ToA nadejścia każdego sygnału, są wyznaczane poprzez poszukiwanie chwil rozpoczęcia tej samej ramki depeszy w każdym z odbieranych sygnałów GPS.



Rysunek 1.1: Zasada określania pozycji w systemie GPS

W systemach GNSS transmitowane są sygnały z bezpośrednio rozproszonym widmem, które są modulowane binarnymi ciągami pseudolosowymi. W przypadku cywilnych sygnałów GPS jest to zbiór 37 ciągów, nazywanych ciągami C/A, stanowiących sekwencje Golda o długości 1023 bitów każda [40]. Ciągi sygnałów militarnych są oznaczone symbolem P(Y). Funkcje autokorelacji ciągów C/A i P(Y) przypominają funkcję autokorelacji szumu, osiągając maksimum w zerze i znacznie mniejsze wartości dla argumentów niezerowych. Pozwala to dokładnie określić chwilę początku ciągu pseudolosowego. Ciąg pseudolosowy C/A powtarzany jest co 1 ms, natomiast szybkość transmisji danych nawigacyjnych wynosi 50 bit/s. Zatem na jeden bit danych przypada dwadzieścia powtórzeń ciągu Golda. Ustalenie chwil czasu, w których rozpoczęto odbiór pierwszego ciągu w określonej ramce danych, umożliwia precyzyjne określenie różnic czasów propagacji sygnałów pochodzących od różnych satelitów.

1.1.2 Czynniki warunkujące dostępność usługi lokalizacyjnej GPS

Niezawodność procesu określania lokalizacji odbiornika GPS jest zdeterminowana przez możliwość ciągłego odbioru prawidłowych sygnałów nawigacyjnych, które przenoszą informacje niezbędne do wyznaczenia położenia. Istnieje wiele czynników, które mogą spowodować, że jakość

wszystkich bądź niektórych docierających do odbiornika sygnałów GPS nie będzie wystarczająca do ich poprawnego odbioru. Spośród tych czynników można wyróżnić m.in.:

- charakter środowiska propagacyjnego: brak bezpośredniej widoczności satelitów (warunki NLoS), propagacja wielodrogowa, zaniki,
- zakłócenia o charakterze naturalnym (zjawiska atmosferyczne),
- niezamierzone zakłócenia spowodowane działalnością człowieka (zakłócenia sąsiedniokanałowe, częstotliwości harmoniczne sygnałów z innych systemów),
- zakłócenia celowe.

Sygnały z rozproszonym widmem charakteryzują się większą odpornością na zaniki i zakłócenia niż sygnały wąskopasmowe o takiej samej szybkości transmisji danych użytkowych. Podczas gdy widmo sygnału użytecznego jest skupiane w odbiorniku GPS, tzn. gdy sygnał jest przekształcany z postaci szerokopasmowej na wąskopasmową, widma zakłóceń wąskopasmowych i zaników selektywnych są rozpraszane, dzięki czemu wywołania nimi degradacja sygnału jest znacząco ograniczona. Dzięki temu, wpływ pierwszych trzech z wymienionych czynników nie jest zwykle na tyle znaczący, aby całkowicie uniemożliwić ustalenie położenia odbiornika. Odrębnie należy potraktować kwestię celowego zakłócania, gdzie sygnał niepożądany, nawet po rozproszeniu jego widma, może znacząco zakłócać sygnał użyteczny [45].

Jest możliwe określenie mocy zakłócenia, które uniemożliwi odbiór jakichkolwiek sygnałów z satelitów GPS. Według oficjalnej specyfikacji interfejsu satelita-odbiornik [29], minimalna moc sygnału GPS z ciągiem C/A (ogólnie dostępnego) na wyjściu anteny odbiorczej powinna wynosić -160 dBW (10^{-16} W). Przy szerokości pasma $B_{C/A}$ sygnału z ciągiem C/A, wynoszącej około 2 MHz, stosunek mocy sygnału do mocy szumu termicznego wynosi -19 dB. Sygnał jest więc odbierany znacząco poniżej poziomu szumów. Miarą jakości odbieranego sygnału GPS jest stosunek $\frac{C}{N_0}$ mocy fali nośnej do widmowej gęstości mocy szumu po skupieniu widma, wyrażony w jednostkach $dBHz$, co można zapisać w następujący sposób:

$$\frac{C}{N_0}\,[dBHz] = 10\log_{10}\left(\frac{C[W]}{N[W]/B[Hz]}\right) = 10\log_{10}\left(\frac{C}{N_0}[Hz]\right). \tag{1.2}$$

Zależność pomiędzy SNR (stosunkiem mocy sygnału C/A do mocy szumu) na wejściu odbiornika a C/N_0 wyraża poniższa zależność:

$$SNR[dB] = \frac{C}{N_0}[dBHz] - 10\log_{10}(B_{C/A}[Hz]) = \frac{C}{N_0}[dBHz] - 63dBHz. \tag{1.3}$$

Wartość progowa $\frac{C}{N_0}$, poniżej której odbiornik GPS nie jest w stanie dokonać poprawnego odbioru sygnału, jest uzależniona od jego czułości i wynosi zwykle nie mniej niż 30 dBHz[1]. Odpowiada to stosunkowi sygnał-szum równemu -33 dB. Zatem, jeśli moc sygnału użytecznego byłaby np. o 10 dB większa od minimalnej i wynosiła -150 dBW, aby go efektywnie zakłócić wystarczyłoby nadać sygnał wąskopasmowy, którego moc na wejściu odbiornika wynosiłaby: -150 $dBW + 33$ $dB = -117$ dBW, czyli ok. $2 \cdot 10^{-12}W$. Moc nadajnika zakłócającego jest oczywiście uzależniona od długości i charakteru trasy propagacji pomiędzy tym nadajnikiem a zakłócanym odbiornikiem. Niemniej jednak, zazwyczaj wystarczający jest nadajnik o stosunkowo małej mocy. Należy także zwrócić uwagę na fakt, że podatność na zakłócenia jest uzależniona od tego, czy w chwili aktywacji sygnału niepożądanego odbiornik jest już dostrojony do sygnału użytecznego (tzn. czy jest w tzw. fazie śledzenia), czy dopiero go poszukuje (faza akwizycji) [46]. Badania opisane w [70] wskazują, że nadajnik, transmitujący sygnał zakłócający z mocą 244 mW, w pasmie o szerokości 2 MHz, jest wystarczający do uniemożliwienia odbioru sygnałów GPS w promieniu ponad 6 km, gdy odbiornik jest dostrojony do sygnałów z satelitów i w promieniu ponad 8 km, gdy odbiornik nie jest jeszcze z nimi zsynchronizowany.

Efektywność zagłuszenia sygnałów GPS nie zależy jedynie od mocy odbieranego sygnału zakłócającego, ale również od jego charakterystyki częstotliwościowej. Widmo impulsów ciągów Golda ma charakter prążkowy, gdzie prążki są oddalone od siebie i od częstotliwości nośnej o wielokrotność 1 kHz, co stanowi odwrotność okresu sekwencji pseudolosowej 1 ms. W publikacji [3] wykazano, że wysoką efektywność zakłócania uzyskuje się poprzez nadawanie sygnałów, których widmowa gęstość mocy jest duża na tych częstotliwościach (np. sygnały mono- i poliharmoniczne). Jedyna trudność realizacji zakłócenia w tym przypadku polega na tym, że częstotliwość nośna sygnału GPS jest przesunięta o częstotliwość Dopplera, której jedna składowa jest

[1] Odbiór sygnałów o mniejszych wartościach $\frac{C}{N_0}$ wymaga zastosowania specjalnych technik uśredniania sygnałów [102]

uzależniona od - w ogólności nieznanej - prędkości satelity względem odbiornika. W badaniach opisanych w [71] wykazano, że silne zakłócenia występujące poza pasmem systemów GNSS mogą również wpływać negatywnie na jakość odbioru sygnałów nawigacyjnych.

Obecnie bez większego problemu można zakupić, m.in. na popularnych internetowych platformach transakcyjnych, urządzenia do zagłuszania GPS montowane w gnieździe zapalniczki samochodowej. Zastosowania tego typu urządzeń są najczęściej niezgodne z prawem, np:

- uniemożliwienie śledzenia przez pracodawcę pozycji pojazdu służbowego,
- zakłócenie pracy systemu automatycznego poboru opłat na autostradach,
- uniemożliwienie wyśledzenia skradzionego pojazdu wyposażonego w lokalizator GPS.

Obecność takich urządzeń zakłócających na rynku wskazuje, że istnieje na nie zapotrzebowanie i że są one w użyciu. Aby przeciwdziałać tego typu aktywnościom, konieczne jest wypracowanie skutecznych metod ich wykrywania i łagodzenia skutków. Dotyczy to szczególnie bardziej wyszukanej formy zakłócania pracy odbiorników GPS, czyli spoofingu, przeciwdziałanie któremu stanowi przedmiot niniejszej rozprawy.

1.2 Charakterystyka spoofingu w systemie GPS

Spoofing (z ang. podszywanie się) można zdefiniować jako rodzaj ataku elektronicznego, który polega na emisji fałszywych sygnałów nawigacyjnych - w tym przypadku GPS - imitujących prawdziwe sygnały docierające do odbiornika z satelitów tego systemu. Urządzenie emitujące tego typu sygnały jest nazywane spooferem. Celem takiego ataku jest doprowadzenie do wyznaczenia przez odbiornik GPS nieprawidłowych informacji o jego pozycji geograficznej, prędkości i czasie. Aby spoofing był skuteczny, moc fałszywych sygnałów na wejściu odbiornika musi większa od mocy sygnałów satelitarnych. Zatem sygnały nadawane w trakcie spoofingu z jednej strony zagłuszają sygnały pożądane, a z drugiej stanowią nośnik nieprawidłowych informacji dla odbiornika znajdującego się w zasięgu spoofera. Wytworzenie sygnałów imitujących te odbierane z satelitów GPS jest możliwe dzięki temu, że pełna informacja o ich strukturze, jak również o postaci wiadomości nawigacyjnych, jest ogólnodostępna, np. w [29]. Do publicznej wiadomości podano wszystkie niezbędne informacje dotyczące sygnałów cywilnych, w tym:

postaci pseudolosowych ciągów rozpraszających, częstotliwości nośne oraz algorytmy kodowania kanałowego. Dane nawigacyjne nie podlegają szyfrowaniu, co istotnie ułatwia sfałszowanie sygnałów.

Spoofer może mieć postać stacji naziemnej, jednakże, z uwagi na możliwość przemieszczania się celu ataku, bardziej prawdopodobne wydają się być scenariusze, w których źródło fałszywych sygnałów znajduje się na pokładzie samolotu, helikoptera, statku lub pojazdu naziemnego. Taki scenariusz utrudnia znalezienie się zakłócanego odbiornika poza zasięgiem spoofera.

Wyróżnia się trzy klasy urządzeń, które mogą zostać użyte do realizacji spoofingu [36, 52, 53]. Różnią się one między sobą: złożonością, kosztem, trudnością zastosowania oraz podatnością na wykrycie. Najłatwiejszy w realizacji scenariusz spoofingu polega na użyciu komercyjnego symulatora konstelacji satelitów GPS. Tego typu urządzenia są produkowane z myślą o wyposażeniu laboratoriów testowania odbiorników GPS, aby zapewnić stabilność i powtarzalność warunków badawczych. Jednakże, gdy na wyjściu takiego generatora zostanie dołączony wzmacniacz mocy oraz antena nadawcza, daje to możliwość transmisji sygnałów GPS o ściśle zdefiniowanej postaci do odbiorników w promieniu wielu kilometrów. Ograniczeniem dostępności generatorów GPS jest ich cena, która nierzadko przekracza wartość 100 tys. złotych. Zazwyczaj przeprowadzenie spoofingu nie wymaga wykorzystania pełnej funkcjonalności takiego generatora. Dlatego też, pod warunkiem posiadania odpowiedniej wiedzy i umiejętności, jest możliwe wykonanie uproszczonego generatora, np. w technice radia programowalnego SDR, co znacząco ogranicza koszty [56]. Podstawowym ograniczeniem zastosowania symulatora GPS w roli spoofera jest brak możliwości zachowania odpowiednich zależności czasowych pomiędzy prawdziwymi a fałszywymi sygnałami. Nie jest to istotne w fazie akwizycji (np. bezpośrednio po włączeniu odbiornika GPS), gdzie następuje zawsze dostrojenie do silniejszego sygnału, ale ma znaczenie w fazie śledzenia, gdy odbiornik jest już dostrojony do prawdziwych sygnałów z satelitów. Aby znacząco zwiększyć szanse powodzenia spoofingu w fazie śledzenia, należałoby zapewnić zgodność: częstotliwości i fazy fali nośnej, fazy ciągu pseudolosowego oraz taktu danych nawigacyjnych pomiędzy sygnałami z satelitów i sygnału spoofera w punkcie odbioru. Jest to spełnione w przypadku użycia bardziej zaawansowanych spooferów.

Urządzenia drugiej klasy stanowią połączenie odbiornika GPS i generatora fałszywych sygnałów [87]. Odbiornik spoofera najpierw dostraja się do prawdziwych sygnałów, pozyskując informację o swojej pozycji, czasie i efemerydach (parametrach orbity) satelitów. Następnie, generator wytwarza fałszywe sygnały o mocach i opóźnieniach dobranych w taki sposób, aby początkowo odpowiadały parametrom uprzednio śledzonych prawdziwych sygnałów z satelitów. Biorąc pod uwagę to, że fałszywe sygnały mają takie same parametry jak prawdziwe, większość prostych metod wykrywania spoofingu jest w tym przypadku bezużyteczna. Pomimo większej skuteczności, trudność w realizacji spoofingu przy użyciu urządzeń tej klasy jest znacznie większa. Przede wszystkim wymagana jest dokładna znajomość odległości pomiędzy zakłócanym odbiornikiem a spooferem. Gdy ma być zachowana zgodność faz fal nośnych, odległość musi być znana praktycznie z dokładnością co do jednego centymetra, co jest możliwe w zasadzie tylko w przypadku gdy oba urządzenia znajdują się np. w tym samym pojeździe. Wykrycie spoofingu realizowanego z użyciem spoofera drugiej klasy jest możliwe m.in. poprzez analizę kierunku nadejścia sygnału DoA , gdyż, w przeciwieństwie do sygnałów odbieranych z satelitów, wszystkie fałszywe sygnały są odbierane z tego samego kierunku.

Trzecia, najbardziej zaawansowana, klasa spooferów ma charakter teoretyczny, gdyż ich zastosowanie w praktyce należy uznać za wysoce nieprawdopodobne. W założeniu, aktywność takich urządzeń jest niewykrywalna przez metodę analizy kierunku nadejścia sygnałów. W tym przypadku spoofer nadaje sygnały nie przez jedną, ale przez wiele anten rozmieszczonych na obszarze wokół zakłócanego odbiornika, co imituje separację przestrzenną satelitów. Każdy z sygnałów musi być opóźniony odpowiednio do aktualnego położenia odbiornika, co, dopuszczając jego poruszanie się, jest zadaniem niemal niemożliwym do wykonania.

Badania prowadzone w Katedrze Systemów i Sieci Radiokomunikacyjnych Politechniki Gdańskiej potwierdzają możliwość skutecznej realizacji spoofingu GPS zarówno przy użyciu komercyjnego generatora sygnałowego, jak również przy użyciu wykonanego w Katedrze generatora opartego o układy programowalne FPGA [47]. Badania nad spoofingiem są prowadzone w wielu ośrodkach badawczych na całym świecie. Badacze z Texas University z Austin w Stanach Zjednoczonych w 2012 roku zaprezentowali możliwość przejęcia kontroli nad autonomicz-

nym bezzałogowym pojazdem latającym, tzw. UAV, korzystającym z nawigacji GPS [88, 89]. Użyto w tym przypadku spoofera drugiej klasy, który dobierał opóźnienia fałszywych sygnałów w oparciu o znajomość prawdziwej pozycji bezzałogowego śmigłowca UAV. Śmigłowiec ten, korzystając z autopilota, miał za zadanie utrzymywać swoją pozycję. Poprzez spoofing doprowadzono do przemieszczenia pojazdu w płaszczyźnie horyzontalnej. Co ciekawe, spowodowano również zmianę jego wysokości, pomimo że bazował on głównie na wysokościomierzu ciśnieniowym, a wysokość odczytana z GPS stanowiła tylko jedną z danych wejściowych rozszerzonego filtru Kalmana. W 2013 r. kontynuacja tych badań pozwoliła uzyskać bardziej szczegółowe wyniki odnośnie działania odbiornika GPS w obecności spoofingu [48]. Także w 2013 roku przeprowadzono eksperyment, w którym z powodzeniem zastosowano spoofing do kontrolowanej zmiany kursu luksusowego jachtu na Morzu Śródziemnym [20]. W publikacjach [37, 90] autorzy wykazali, że spoofing GPS może także zakłócić pracę wzorców czasu stosowanych w sieciach elektroenergetycznych przy monitorowaniu fazy prądu i napięcia. Dopuszczalny błąd pomiaru tych faz wynosi 0,573°. Tymczasem wyniki pomiarów przeprowadzonych podczas realizacji spoofingu wskazały wartości tego błędu wynoszące nawet kilkadziesiąt stopni.

W przeciwieństwie do zagłuszania sygnałów GPS, trudno jest znaleźć doniesienia o przypadkach zastosowania spoofingu innych niż eksperymenty naukowe. W grudniu 2011 roku na terenie Iranu doszło do przechwycenia amerykańskiego drona (bezzałogowego samolotu) poprzez zakłócenie jego systemów nawigacyjnych i sprowadzenie na ziemię. Według Irańczyków, został przeprowadzony spoofing sygnałów GPS przy jednoczesnym zagłuszeniu łącza służącego do zdalnego sterowania dronem. Wprawdzie, jako urządzenie armii USA, odbiornik GPS samolotu najprawdopodobniej korzystał z, praktycznie niemożliwych do sfałszowania, sygnałów militarnych GPS, modulowanych ciągiem P(Y), jednakże, gdy zostały one zakłócone przez spoofing, mógł opierać się na nieprawidłowych (fałszywych) sygnałach cywilnych C/A.

1.3 Cel i teza rozprawy

Na podstawie powyższego opisu można wysnuć wniosek, że spoofing jest realnym zagrożeniem i koniecznym jest podjęcie działań, mających na celu "uodpornienie" odbiorników GPS na tego typu ataki. Celem niniejszej pracy jest opracowanie niezawodnych metod wykrywania i eliminacji spoofingu GPS oraz zbadanie efektywności systemu antyspoofingowego, stanowiącego realizację tych metod w strukturze odbiornika nawigacyjnego.

Wyznacznikiem efektywności metody wykrywania spoofingu jest, z jednej strony, zakres scenariuszy, w których można zastosować daną metodę, a z drugiej prawdopodobieństwo wykrycia ataku w zależności od niepewności parametru decyzyjnego. Z kolei metody eliminacji mogą być oceniane z punktu widzenia maksymalnego stosunku mocy sygnału spoofera do mocy sygnału z satelity, przy którym jest możliwe zapewnienie poprawnego odbioru sygnału pożądanego. Ponadto, istotny jest stopień degradacji sygnałów użytecznych, towarzyszącej eliminacji sygnału spoofera. Oczywiście powinien być on możliwie jak najmniejszy.

W następnym rozdziale tej rozprawy dokonano analizy stanu wiedzy dotyczącej znanych metod wykrywania i eliminacji spoofingu. Następnie, mając na uwadze wady i zalety istniejących rozwiązań, zaproponowano nową koncepcję systemu antyspoofingowego, funkcjonującego w oparciu o przestrzenne przetwarzanie odbieranych sygnałów GPS. Zbadanie efektywności metod zastosowanych w tym systemie jest niezbędne do stwierdzenia, czy może być on z powodzeniem użyty do przeciwdziałania spoofingowi. Stanowi to podstawowy problem naukowy, którego rozwiązania podjęto się w niniejszej pracy.

W związku z powyższym, sformułowano następującą tezę niniejszej rozprawy doktorskiej: **Przy zastosowaniu odbioru wieloantenowego jest możliwe wykrycie spoofingu GPS, polegającego na emisji imitacji sygnałów systemu GPS przez urządzenie zwane spooferem. Ponadto, poprzez zastosowanie filtracji przestrzennej, jest możliwe ograniczenie wpływu sygnałów nadawanych przez spoofer na pracę odbiornika GPS.**

W celu dowiedzenia słuszności powyższej tezy, przeprowadzono szereg badań. Wstępnej oceny efektywności proponowanego systemu dokonano na podstawie wyników badań symula-

cyjnych. Dla przyjętej metody wykrywania zostało zdefiniowane kryterium detekcji spoofingu, a następnie zostało oszacowane prawdopodobieństwo detekcji przy ustalonym prawdopodobieństwie fałszywego alarmu i przy różnych charakterystykach zmienności parametru decyzyjnego. W przypadku metody eliminacji spoofingu, określono możliwe do uzyskania tłumienie sygnałów spoofera oraz prawdopodobieństwo tego, że zostanie uniemożliwiony odbiór określonej liczby sygnałów użytecznych, docierających z satelitów systemu GPS.

Oprócz badań symulacyjnych, efektywność systemu antyspoofingowego, w którym znajdują zastosowanie przyjęte metody, zweryfikowano na drodze badań pomiarowych w warunkach laboratoryjnych i rzeczywistych. W badaniach pomiarowych m.in. zweryfikowano charakterystyki prawdopodobieństwa detekcji spoofingu, a także zbadano poprawność wyznaczania zbioru fałszywych sygnałów oraz określono wpływ eliminacji spoofingu na wartości $\frac{C}{N_0}$ fałszywych i prawdziwych sygnałów GPS.

Rozdział 2

Wykrywanie i przeciwdziałanie spoofingowi GPS

Pierwsza część tego rozdziału zawiera studium i podsumowanie stanu wiedzy dotyczącego metod detekcji spoofingu. Metody te bazują na kryteriach, które oferują różne poziomy skuteczności wykrywania spoofingu. Różnice występują również w kwestii złożoności praktycznej implementacji tych metod.

W kolejnej części rozdziału zestawiono istniejące koncepcje eliminacji wpływu odbieranych fałszywych sygnałów GPS na możliwość odbioru sygnałów prawdziwych. Eliminacja ma na celu umożliwienie poprawnej nawigacji z użyciem odbiornika znajdującego się w zasięgu sygnałów spoofera.

Na podstawie dokonanej analizy, stwierdzono, że największą niezawodnością charakteryzują się metody wykrywania i eliminacji spoofingu bazujące na parametrach przestrzennych odbieranych sygnałów. W związku z tym, w trzeciej części rozdziału, przedstawiono w sposób szczegółowy podstawy teoretyczne funkcjonowania tych metod.

W ostatnim punkcie tego rozdziału zaproponowano zbiór parametrów, które stanowią kryteria oceny metod wykrywania i eliminacji spoofingu. Zbiór takich parametrów nie został

dotychczas ściśle określony w jakiejkolwiek spośród publikacji, z których treścią zapoznał się autor niniejszej rozprawy.

2.1 Analiza porównawcza metod wykrywania spoofingu

Jedną z pierwszych publikacji, w których wskazano zagłuszanie i spoofing, jako potencjalne zagrożenia dla funkcjonowania systemu GPS, jest raport instytutu Volpe'a [95]. Od chwili jego opublikowania podejmowano działania, mające na celu opracowanie skutecznych metod wykrywania obecności fałszywych sygnałów GPS. Spośród szeregu artykułów traktujących o tej tematyce, można wyróżnić [96], opublikowany w dwa lata po wspomnianym raporcie. Bardziej aktualne i szczegółowe zestawienia sposobów przeciwdziałania spoofingowi można znaleźć m.in. w [36, 84]. Wynika z nich, że sygnały spoofera mogą oddziaływać na odbiornik GPS na trzech poziomach, a mianowicie: na poziomie przetwarzania sygnałów, na poziomie analizowania treści depesz nawigacyjnych oraz na poziomie wyznaczania położenia odbiornika. Na pierwszym, najniższym poziomie, fałszywe sygnały, których moc przewyższa moc sygnałów z satelitów, wpływają na układ automatycznej regulacji wzmocnienia. Powoduje to degradację prawdziwych sygnałów, polegającą na zmniejszeniu stosunku ich mocy do mocy szumów własnych odbiornika i szumu kwantyzacji. Znamienne jest także to, że dokładne informacje o strukturze sygnałów GPS, tj.: rodzaj modulacji, postaci ciągów pseudolosowych, częstotliwości nośne, szerokości pasm i zakresy częstotliwości Dopplera, są powszechnie znane, co znacząco ułatwia spreparowanie imitacji prawdziwych sygnałów.

Drugą płaszczyzną oddziaływania spoofingu jest treść depeszy nawigacyjnej, która nie podlega szyfrowaniu, a jej postać ramkowa także jest powszechnie znana. Ponadto, zawartość nadawanych przez satelity wiadomości zmienia się stosunkowo rzadko. Zatem odtworzenie i modyfikacja ramki danych przez spoofer nie nastręcza większych trudności.

Najwyższym poziomem przetwarzania w odbiorniku, na który wpływa spoofing jest procedura wyznaczania położenia. W tym przypadku, modyfikacja pseudoodległości, przy niezmienionych parametrach sygnałów i zawartościach depesz nawigacyjnych, może spowodować wyznaczenie błędnej pozycji i prędkości odbiornika GPS. Podatność na tego typu modyfikację jest

szczególnie wysoka w przypadku niekorzystnej geometrii satelitów względem odbiornika, tzn. gdy wartość parametru PDOP jest duża [39].

Aby mieć możliwość ochrony odbiornika przed działaniem spoofingu, należy najpierw wykryć jego obecność. Podstawowym problemem wykrywania spoofingu jest to, w jaki sposób można odróżnić sygnały prawdziwe od sfałszowanych. W publikacjach poruszających zagadnienie spoofingu można znaleźć wiele propozycji sposobów wykrywania transmisji fałszywych sygnałów GNSS. Prezentowane rozwiązania różnią się w kwestiach złożoności sprzętowej i obliczeniowej oraz oferowanej skuteczności detekcji.

Najprostsze metody wykrywania spoofingu bazują na monitorowaniu wartości podstawowych parametrów odbieranych sygnałów GPS, co wymaga jedynie niewielkiego rozszerzenia funkcjonalności oprogramowania odbiornika. Zazwyczaj obserwowane wielkości są związane z mocą sygnałów na wejściu odbiornika. Z uwagi na, z reguły nieznaną, wartość tłumienia na trasie propagacji sygnału pomiędzy spooferem a odbiornikiem, moc nadawanych sygnałów fałszywych najczęściej znacznie przewyższa moc sygnałów z satelitów GPS. Zatem można podejrzewać obecność spoofingu w sytuacji, gdy moc bezwzględna odbieranych sygnałów jest zbyt duża (np. znacząco przekracza -153 dBW w pasmie L1), aby mogły one pochodzić z satelity oddalonego o tysiące kilometrów. Jeśli dysponuje się odbiornikiem dwuczęstotliwościowym, można zmierzyć stosunek mocy sygnałów odbieranych na częstotliwościach L1 i L2, który jest równy 6 dB po stronie nadawczej. Po stronie odbiorczej stosunek ten może być nieco inny, m.in. z uwagi na refrakcję jonosferyczną [97], jednak znaczące odchylenie od tej wartości może wskazywać na obecność spoofingu. Ponadto, w normalnych warunkach, sygnały docierające z satelitów mają różne moce, które są wolnozmienne w czasie wskutek ruchu satelitów. Natomiast moce odbieranych sygnałów fałszywych często oscylują wokół ustalonej wartości, jeśli odbiornik nie zmienia swojego położenia względem spoofera. Z uwagi na zastosowanie wielodostępu CDMA i współużytkowanie tych samych pasm częstotliwości przez wszystkie satelity w systemie GPS, bezpośredni pomiar mocy sygnałów z różnych satelitów nie jest możliwy i należy w tym przypadku posługiwać się stosunkiem $\frac{C}{N_0}$, wyznaczanym już po skupieniu widma. Jeśli w długim przedziale czasu wartość tego parametru dla odbieranych sygnałów jest niezmienna, zachodzi

podejrzenie obecności spoofingu. Także zaobserwowanie sytuacji skokowej zmiany mocy sygnału lub $\frac{C}{N_0}$ może budzić podejrzenia nieprawidłowości. Jeśli odbiornik GPS się porusza, o obecności spoofingu można wnioskować na podstawie zmian mocy sygnału w funkcji położenia. Gdy sygnał jest odbierany z satelity, przy braku lub niewielkim wpływie propagacji wielodrogowej, ruch odbiornika nie wpływa istotnie na moc sygnału. Z kolei moc sygnału fałszywego jest odwrotnie proporcjonalna do kwadratu odległości od spoofera. Zatem, jeśli spoofer znajduje się stosunkowo blisko odbiornika, zmiana położenia tego ostatniego wywoła znaczącą zmianę poziomu sygnału. Nie dotyczy to oczywiście sytuacji, gdy spoofer i zakłócany odbiornik znajdują się w tym samym pojeździe.

Wymienione powyżej metody są nieskomplikowane i nie wymagają znaczącej modyfikacji odbiorników GPS. Należy jednakże zauważyć, że są one skuteczne jedynie w ograniczonej liczbie scenariuszy. Mogą nie być odpowiednie np. gdy spoofer generuje sygnały w pasmach L1 i L2 oraz dokonuje zmian mocy w czasie niezależnie dla każdego sygnału składowego C/A (sygnału powiązanego z pojedynczym satelitą).

Oprócz śledzenia parametrów związanych z mocą sygnałów, można również obserwować zależności czasowe. Specyfikacja sygnałów GPS określa, że szybkość transmisji depeszy nawigacyjnej jest równa 50 bitów na sekundę, zatem zmiana stanu logicznego występuje w odstępach równych wielokrotnościom 20 ms.[1] Jeśli spoofer nie jest zsynchronizowany z sygnałami prawdziwymi, odbiornik GPS może wykryć nieprawidłową chwilę wystąpienia zmiany bitu i podjąć na tej podstawie decyzję o wykryciu spoofingu. Jeśli dysponuje się odbiornikiem dwuczęstotliwościowym, można zmierzyć, poprzez funkcję korelacji skrośnej, wzajemne opóźnienie sygnałów w pasmach L1 i L2. Gdy spoofer wytwarza sygnał jedynie w pasmie L1, gdzie przesyłany jest sygnał cywilny, wzajemne opóźnienie będzie znacząco odbiegać od obserwowanego w normalnych warunkach. Także wynik bezpośredniego pomiaru opóźnienia jonosferycznego będzie się istotnie różnił od wartości obliczonej w oparciu o model Klobuchara [50].

Innym kryterium, które umożliwia odróżnienie sygnałów prawdziwych od sfałszowanych jest kierunek ich nadejścia. Spoofer nadaje wszystkie sygnały poprzez jedną antenę nadawczą,

[1] W rzeczywistości odstęp ten może być nieznacznie krótszy lub dłuższy, z uwagi na zjawisko Dopplera

zatem docierają one do odbiornika z tego samego kierunku, jako sygnał bezpośredni lub odbity. Z kolei kierunki nadejścia prawdziwych sygnałów, pochodzących z nadajników umieszczonych na satelitach GPS, są różne i nieustannie się zmieniają na skutek ruchu satelitów względem odbiornika. Porównanie kierunków nadejścia wszystkich odbieranych sygnałów GPS daje podstawę do wykrycia spoofingu. Jest również możliwe sprawdzenie, czy wyznaczone kierunki odpowiadają bieżącemu rozmieszczeniu konstelacji satelitów [66]. Estymacja kierunku nadejścia sygnału jest zazwyczaj realizowana z użyciem szyku antenowego, jednakże, w przypadku gdy odbiornik się przemieszcza, szyk antenowy można zastąpić pojedynczą anteną (metoda tzw. syntetycznej apertury) [73]. Proponowane są także rozwiązania, w których sama antena odbiornika jest celowo wprawiana w ruch np. oscylacyjny i są analizowane przebiegi zmian faz fal nośnych sygnałów różnych satelitów w funkcji położenia anteny [82]. W przypadku sygnałów spoofera przebiegi te są niemal identyczne.

W literaturze opisywane są także metody detekcji spoofingu oparte na analizie przebiegu na wyjściu korelatora w odbiorniku GPS [13]. Korelator stanowi blok odbiornika GPS, w którym jest obliczana funkcja korelacji sygnału odbieranego z jego lokalnie wytworzoną repliką. Znajomość wartości funkcji korelacji umożliwia zapewnienie synchronizacji ciągu C/A w odbiorniku, co jest wymagane do skupienia widma sygnału. Metody wykrywania spoofingu w oparciu o wartości z wyjścia korelatora zakładają, że ciągi pseudolosowe sygnałów spoofera są początkowo zsynchronizowane z odpowiednimi ciągami występującymi w prawdziwych sygnałach GPS. Często rozwiązania tego typu wywodzą się z prac poświęconych przeciwdziałaniu zjawisku wielodrogowości w systemie GPS [14, 21]. Odbiór sygnałów spoofera, podobnie jak występowanie odbić prawdziwych sygnałów GPS, wpływa na kształt wyznaczonego przebiegu funkcji korelacji. Jedna z takich metod, nazwana metodą monitorowania jakości sygnału (SQM) [77] została zaadaptowana do wykrywania spoofingu w odbiornikach, do których sygnał z satelitów GPS dociera bezpośrednio (warunki LoS). Decyzja o wykryciu jest, w tym wypadku, podejmowana na podstawie analizy asymetrii i spłaszczenia przebiegu funkcji korelacji wokół jej maksimum [76]. Inna metoda z tej grupy bazuje na analizie rozkładu próbek z wyjścia korelatora. W normalnych warunkach rozkład ten przypomina dystrybucję chi-kwadrat (χ^2). Jeśli zaobserwowany

jest rozkład od niej odbiegający, wskazuje to na możliwość spoofingu. Proponowana jest również metoda, w której detekcja spoofingu jest oparta na korelacji sygnałów z wejść dwóch odbiorników GPS, przy czym jeden z nich musi znajdować się w miejscu, co do którego jest pewność, że nie występuje w nim spoofing [81].

Skutecznym sposobem wykrywania nieprawidłowości w odbieranym sygnale GPS może być porównanie wyznaczonego położenia odbiornika z położeniem ustalonym w oparciu o dane z innego systemu lokalizacyjnego, np. naziemnego eLoran [38] lub systemów inercyjnych [31, 74]. Wadą takiego rozwiązania jest większy koszt (dwa odbiorniki lub odbiornik zintegrowany) Ponadto, korzystanie z innych systemów nawigacyjnych wiąże się z ograniczeniami. Sygnały naziemnych systemów radionawigacyjnych mogą być odbierane tylko na określonym obszarze. Z kolei w systemach inercyjnych problem stanowi kumulacja błędu estymacji położenia [75].

Niektóre spoofery, zwłaszcza te mniej wyszukane, mogą wytwarzać sygnały o strukturze wykazującej pewne nieprawidłowości, które jednakże nie są krytyczne z punktu widzenia możliwości wyznaczenia pozycji przez odbiornik. Przykładowo, w prawdziwym sygnale GPS występuje ścisła zależność pomiędzy odchyłką Dopplera fali nośnej a szybkością zmiany fazy ciągu pesudolosowego. Ta zależność może nie być spełniona w przypadku sygnałów fałszywych. Może także nie być zachowana spójność danych pomiędzy depeszą nawigacyjną a aktualnie udostępnianymi informacjami o położeniu satelitów, lub też nawet zachodzić brak spójności danych efemerydalnych lub danych o taktach zegarów poszczególnych satelitów. W takich przypadkach podatność odbiornika na spoofing zależy od tego, jak szczegółowe są algorytmy sprawdzania zgodności struktury odbieranych sygnałów ze specyfikacją interfejsu satelita-odbiornik [29].

Niektórzy autorzy postulują wprowadzenie zabezpieczenia kryptograficznego do obecnych i przyszłych sygnałów GPS, jako formę ochrony przed ich fałszowaniem [33, 51, 80]. Jest oczywistym, że przy modyfikacji struktury sygnałów należy zachować kompatybilność wsteczną ze wszystkimi dotychczas wyprodukowanymi odbiornikami. Jednym z takich rozwiązań jest użycie aktualnie niewykorzystanych pól depeszy nawigacyjnej do przesyłania podpisanego cyfrowo skrótu wiadomości [16]. Inna propozycja zakłada połączenie ochrony kryptograficznej z analizą parametrów czasowych sygnałów [100]. Szyfrowanie może obejmować zarówno depeszę nawiga-

cyjną, jak i ciągi pseudolosowe C/A [88, 101], niemniej to drugie rozwiązanie jest mniej preferowane z uwagi na większy koszt budowy odbiornika [79]. Należy jednakże brać pod uwagę, że jakakolwiek modyfikacja postaci nadawanych sygnałów GPS wymaga odgórnego działania rządu USA w tym obszarze, co nie jest konieczne w przypadku wcześniej wymienionych metod wykrywania spoofingu, zakładających modyfikacje wyłącznie po stronie odbiornika.

Tabela 2.1: Porównanie metod wykrywania spoofingu GPS

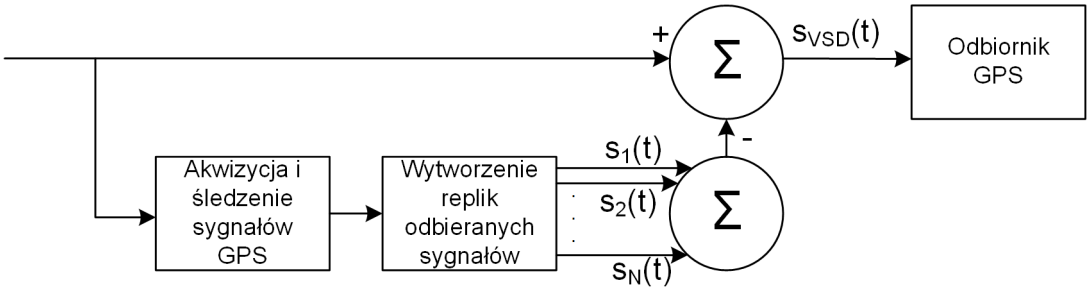
L.p.	Metoda	Złożoność	Skuteczność
1	Monitorowanie C/N_0	Mała	Średnia
2	Monitorowanie mocy bezwzględnej	Mała	Średnia
3	Zmiana mocy w funkcji ruchu odbiornika	Mała	Mała
4	Porównanie mocy w pasmach L1 i L2	Mała	Średnia
5	Porównanie kierunku nadejścia sygnału (szyk antenowy)	Duża	Duża
6	Porównanie kierunku nadejścia sygnału (apertura syntetyczna)	Mała	Duża
7	Pomiar czasu pomiędzy zmianami bitu	Średnia	Średnia
8	Pomiar opóźnienia L1 i L2	Średnia	Średnia
9	Monitorowanie jakości sygnału (SQM)	Średnia	Średnia
10	Analiza rozkładu próbek z wyjścia korelatora	Mała	Średnia
11	Porównanie z innym systemem nawigacyjnym	Duża	Duża
12	Porównanie szybkości zmian fali nośnej i ciągu PRN	Mała	Mała
13	Sprawdzanie spójności danych efemeryd i zegara	Mała	Średnia
14	Zabezpieczenie kryptograficzne depeszy	Duża	Duża

W Tab. 2.1 porównano wszystkie wyżej wymienione metody wykrywania spoofingu GPS, mając na uwadze ich złożoność sprzętowo-obliczeniową oraz skuteczność detekcji. Na podstawie tego zestawienia można wysnuć wniosek, że największą skutecznością cechują się metody o numerach 5, 6, 11 i 14. Jednakże, zakres stosowalności dwóch ostatnich jest znacznie ograniczony. Wynika stąd, że najlepszym wyborem metody wykrywania spoofingu, pomijając kwestię złożoności jej implementacji, jest użycie jednej z metod 5 lub 6, bazujących na analizie przestrzennej odbieranych sygnałów.

2.2 Metody eliminacji spoofingu

W sytuacji gdy spoofing GPS zostanie wykryty, powinny zostać podjęte kroki, mające na celu zminimalizowanie jego oddziaływania i zapobiegnięcie potencjalnie niebezpiecznym sytuacjom, które mogłyby być nim wywołane. Najprostszym sposobem jest powiadomienie użytkownika o zaistnieniu faktu odbioru fałszywych sygnałów, pozostawienie odbiornika w trybie monitorowania obecności spoofingu oraz czasowe zaprzestanie wyznaczania położenia, prędkości i czasu. Powrót do normalnej pracy byłby możliwy w przypadku wykrycia wyłączenia spoofera lub znalezienia się odbiornika poza jego zasięgiem. Takiego rozwiązania nie można jednakże zastosować w przypadkach, gdzie długotrwałe przerwy w dostępności sygnałów GPS mogłyby spowodować nieprawidłowe działanie urządzeń lub systemów. Dlatego też poszukiwane są metody przeciwdziałania spoofingowi w taki sposób, aby, pomimo występowania tego celowego zakłócenia, umożliwić odbiór prawdziwych sygnałów GPS.

W odróżnieniu od mnogości proponowanych w literaturze metod detekcji spoofingu, niewiele jest znanych sposobów jego eliminacji. Wynika to z ograniczonych możliwości fizycznego odseparowania sygnałów fałszywych i prawdziwych tak, aby eliminacja tych pierwszych nie uniemożliwiła jednocześnie odbioru drugich. W przypadku, gdy sygnały GPS podlegają zakłóceniom wąskopasmowym lub impulsowym, można zastosować filtrację bezpośrednio w dziedzinie czasu lub częstotliwości. Znane są także metody filtracji z użyciem transformacji falkowej [22]. Jednakże, w przypadku gdy sygnał zakłócający jest szerokopasmowy i niemal identyczny z sygnałem użytecznym, takie operacje są nieefektywne.



Rysunek 2.1: Metoda wykrywania sygnału resztkowego (VSD)

Warunkiem koniecznym powodzenia spoofingu jest przewaga mocy sygnałów fałszywych, w stosunku do mocy sygnałów pochodzących z satelitów. Stosunek mocy powinien być z jednej strony na tyle duży, aby zakłócić sygnały prawdziwe, a z drugiej strony na tyle mały, aby spoofing nie został łatwo wykryty z użyciem metod opartych na analizie mocy lub $\frac{C}{N_0}$ odbieranych sygnałów. Takim założeniem kierowali się twórcy metody przeciwdziałania spoofingu nazywanej wykrywaniem sygnału resztkowego VSD [98]. Schemat blokowy tej metody został przedstawiony na Rys. 2.1. Zasada jej działania polega na tym, że od całego sygnału na wyjściu anteny odbiornika są odejmowane odtworzone repliki, uznanych za fałszywe, odbieranych sygnałów GPS o dużej mocy. Wynik takiej operacji powinien odpowiadać sygnałowi odbieranemu przy braku spoofingu. Po odjęciu replik sygnałów nadawanych przez spoofer, można poszukiwać prawdziwych sygnałów GPS, których pierwotne wykrycie było niemożliwe z uwagi na ich zbyt małą moc . Problem w przypadku tej metody może pojawić się w sytuacji, gdy, np. na skutek zmiany położenia odbiornika, moc sygnałów fałszywych będzie mniejsza niż moc sygnałów odbieranych z satelitów. Istnieje wtedy ryzyko, że to prawdziwe sygnały będą odrzucone na rzecz fałszywych. W innym przypadku, gdy moc sygnałów spoofera znacząco wzrośnie, co wywoła spadek wzmocnienia w pętli ARW, odbiór sygnałów prawdziwych może być niemożliwy z uwagi na szum kwantyzacji. Problem przesterowania układu ARW w odbiornikach GNSS został opisany w [5].

Inną metodą eliminacji spoofingu GPS jest rozwiązanie o nazwie RAIM (Receiver Autonomous Integirty Monitoring). Jest to technika stosowana obecnie w niektórych odbiornikach GPS do wykrywania nieprawidłowości w odbieranych sygnałach, co może być spowodowane np. awarią satelity. Podstawą do aktywacji alarmu w odbiorniku i wykluczenia danego satelity z procedury wyznaczania pozycji jest niespójność depeszy nawigacyjnej lub niespójność pseudoodległości z tymi, które są określone dla pozostałych satelitów. W przypadku gdy aktywność spoofera uniemożliwia odbiór poprawnych depesz i pomiar właściwych pseudoodległości od satelitów, można porównywać pomiary bieżące z poprzednimi w celu wykrycia nagłych, nieoczekiwanych zmian w odbieranych sygnałach.

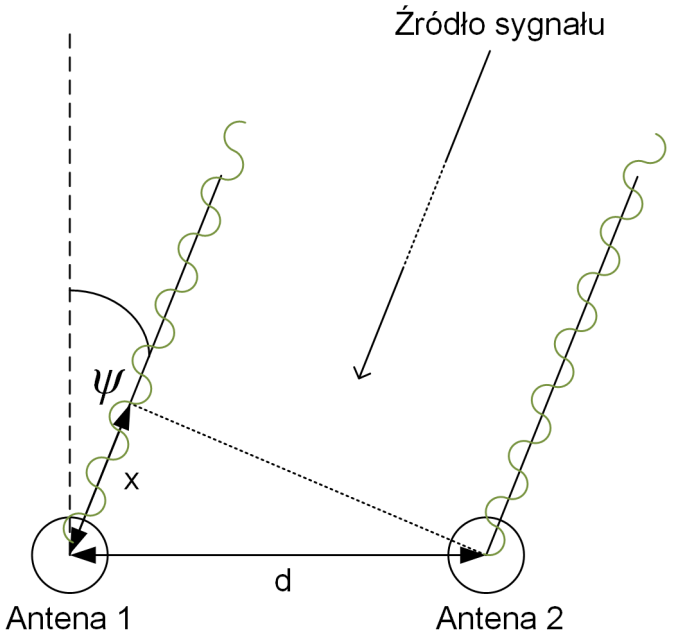
RAIM może zostać użyty do wykrycia spoofingu w części przypadków, gdy fałszywe sygnały nie są zsynchronizowane z prawdziwymi. Jednakże, w 2008 roku, na Uniwersytecie w Austin

w Teksasie, opracowano spoofer drugiej klasy, który umożliwia nadawanie sygnałów zgodnych w czasie, częstotliwości i fazie z prawdziwymi sygnałami na wejściu anteny odbiornika GPS [35]. Tego typu spoofer, dzięki zwiększaniu mocy wyjściowej, powoduje płynne i niezauważalne dla użytkownika przejęcie kontroli nad wskazaniami odbiornika. W drugiej fazie spoofingu, specjalnie spreparowane sygnały powodują, że pozycja wskazywana przez odbiornik stopniowo coraz bardziej odbiega od prawdziwej. W przypadku takiego scenariusza, w żadnej chwili nie jest możliwe wykrycie niespójności w zbiorze odbieranych sygnałów GPS, czego rezultatem jest nieskuteczność techniki RAIM.

Trzecim sposobem rozwiązania problemu ze spoofingiem jest przestrzenne przetwarzanie sygnałów. W tym przypadku bazuje się na tym, że wszystkie fałszywe sygnały docierają do odbiornika z tego samego kierunku. Poprzez odpowiednie ukształtowanie charakterystyki anteny odbiorczej, można stłumić odbiór sygnałów docierających z jednego lub kilku kierunków, jednocześnie nie powodując istotnej degradacji sygnałów o innych kątach nadejścia. Aby uzyskać możliwość adaptacyjnej filtracji przestrzennej, należy zastosować szyk antenowy, czyli układ złożony z co najmniej dwóch, najczęściej takich samych, odbiorczych elementów antenowych. Elektroniczna kontrola kształtu charakterystyki szyku jest realizowana poprzez jego fazowanie, czyli modyfikację faz i amplitud sygnałów z wyjść poszczególnych elementów antenowych. Biorąc pod uwagę fakt, że aktualnie spoofery nie są na tyle zaawansowane, żeby imitować różne kierunki nadejścia sygnału (spoofery trzeciej klasy), filtracja przestrzenna jest obecnie postrzegana jako najbardziej efektywny sposób walki ze spoofingiem GPS.

2.3 Przetwarzanie przestrzenne sygnałów spoofera

Zgodnie z treścią powyższego opisu, metody przestrzennego przetwarzania sygnałów mogą znaleźć zastosowanie zarówno w wykrywaniu, jak i w eliminacji spoofingu. Ochrona odbiornika GPS, bazująca na analizie kierunku nadejścia sygnału, jest trudna do pokonania, nawet przez zaawansowane spoofery drugiej klasy. W związku z tym, zdecydowano, że, proponowana w niniejszej rozprawie, koncepcja kompleksowego systemu antyspoofingowego GPS będzie również oparta na algorytmach przestrzennego przetwarzania sygnałów. Poniżej zawarto bardziej szczegółowy opis teoretyczny, dotyczący estymacji kierunku nadejścia sygnału i filtracji przestrzennej.



Rysunek 2.2: Interferometria fazowa z użyciem dwóch anten

2.3.1 Wykrywanie spoofingu

Jak wspomniano w podrozdziale 2.1, wykrycie spoofingu jest możliwe w oparciu o porównanie kierunków nadejścia sygnałów GPS. Technika określania kierunku nadejścia jest rozwijana od początku dwudziestego wieku. Pierwotnie, w tym celu były stosowane odbiorcze anteny kierunkowe, które były obracane i wskazywały kierunek do źródła sygnału w chwili, gdy moc na ich wyjściu osiągała wartość maksymalną. W dzisiejszych czasach określanie kierunku jest zazwyczaj związane z pomiarami przesunięcia fazowego lub odchyłki Dopplera częstotliwości nośnej. Stosowane są również metody bazujące na analizie podprzestrzeni wektorowych sygnału i szumu (ang. subspace-based), jak np. algorytm MUSIC [92]. Estymują one kierunek nadejścia sygnału (DoA) w oparciu o analizę kowariancji kilku kopii tego sygnału, odbieranych przez przez różne elementy układu antenowego. Wiele z metod określania DoA jest używanych do namierzania sygnałów o nieznanych parametrach, w związku z czym często nie uwzględniają one informacji o strukturze sygnału w celu poprawy jakości estymacji. Ponadto, do ich prawidłowego działania

jest wymagany duży stosunek mocy sygnału do szumu, co jest spełnione głównie w przypadku transmisji wąskopasmowych. Cywilne sygnały GPS, o szerokości pasma przekraczającej 2 MHz, docierają do odbiornika z bardzo małą mocą, która może być prawie 100 razy mniejsza od mocy szumu termicznego. Dodatkowo, sygnały wszystkich satelitów GPS współdzielą to samo pasmo częstotliwości (wielodostęp CDMA), co utrudnia powiązanie kierunku nadejścia z konkretnym numerem satelity. Pomimo tego, metody MUSIC i jej podobnych można użyć do estymacji kierunku nadejścia sygnału w odbiorniku systemu GPS. Jednakże, jest to możliwe dopiero na etapie przetwarzania sygnałów, który następuje po operacji skupiania widma. W trakcie tej operacji są wyodrębniane sygnały pochodzące od poszczególnych satelitów GPS.

Kierunek nadejścia sygnału można określić na podstawie pomiarów względnych opóźnień fazowych sygnału na wejściach elementów szyku antenowego. Nosi to nazwę interferometrii fazowej [99]. W najprostszym przypadku, przedstawionym na Rys. 2.2, przy użyciu dwóch anten, jest możliwe określenie kąta nadejścia sygnału w jednej płaszczyźnie, w zakresie $\pm 90°$. Zależność pomiędzy kątem nadejścia sygnału ψ a opóźnieniem fazowym $\Delta\phi_{1,2}$ wyraża się następująco:

$$\psi = arcsin\left(\frac{\lambda\Delta\phi_{1,2}}{2\pi d_{1,2}}\right), \tag{2.1}$$

gdzie λ jest długością fali, a $d_{1,2}$ jest odległością pomiędzy elementami antenowymi. Dwuelementowy układ antenowy charakteryzuje się ograniczonymi możliwościami wyznaczania kierunku nadejścia sygnału. Po pierwsze, opóźnienia fazowe są symetryczne względem linii przechodzącej przez środki anten, zatem występuje niejednoznaczność co do tego, z której strony tej linii sygnał dociera do układu. Po drugie, jest tylko jeden stopień swobody, zatem można wyznaczyć jedynie np. kąt azymutu przy ustalonym kącie elewacji. Rozwiązaniem tych problemów są bardziej rozbudowane układy antenowe.

Również dla szyków antenowych o większej liczbie elementów, można wyprowadzić równania analogiczne do (2.1), definiujące zależności pomiędzy opóźnieniami fazowymi a kątami opisującymi kierunek nadejścia sygnału. Są to równania zawierające funkcje trygonometryczne, w związku z czym są one nieliniowe. Sprawia to, że wielkość błędu estymacji kierunku nadejścia sygnału jest uzależniona od tego, pod jakim kątem ten sygnał dociera do odbiornika. W praktyce

oznacza to, że prawdopodobieństwo wykrycia spoofingu będzie zależeć od wzajemnej orientacji przestrzennej spoofera względem elementów odbiorczego szyku antenowego. Z tego względu zdecydowano, że, w proponowanym systemie antyspoofingowym, o wykryciu spoofingu nie będą decydować różnice kierunków nadejścia sygnałów o różnych ciągach C/A. Zamiast tego, aby wyeliminować nieliniowość błędu estymacji, będą analizowane różnice, zmierzonych pomiędzy wybranymi elementami szyku, opóźnień fazowych tych sygnałów. Układ decyzyjny wykryje obecność spoofingu, gdy wszystkie różnice opóźnień fazowych sygnałów o różnych ciągach C/A będą mniejsze niż ustalona wartość progowa. Prawidłowy dobór progu detekcji powinien uwzględniać liczbę odbieranych sygnałów oraz ich jakość, wyrażoną wartością parametru $\frac{C}{N_0}$.

2.3.2 Eliminacja spoofingu - filtracja przestrzenna

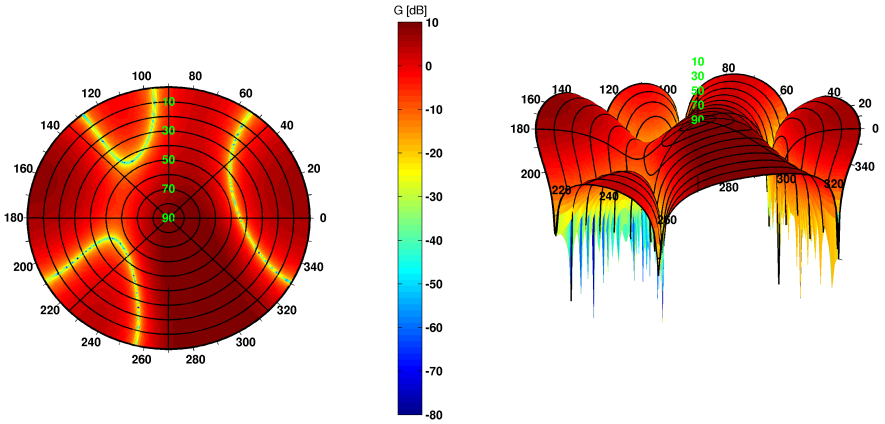
Kształt charakterystyki szyku antenowego jest uzależniony od wartości liczb, stanowiących tzw. współczynniki wagowe, przez które są mnożone sygnały z wyjść poszczególnych elementów antenowych. Najczęściej są to liczby zespolone, choć spotykane są także rozwiązania bazujące na liczbach rzeczywistych [93]. Zbiór współczynników jest nazywany wektorem wagowym. Istnieje wiele metod doboru takich postaci wektora wagowego, które pozwalają zmaksymalizować wyjściowy stosunek mocy sygnału użytecznego do mocy sygnałów niepożądanych. Możliwość zastosowania poszczególnych metod jest uzależniona od ilości dostępnej informacji o parametrach sygnałów użytecznych i zakłócających.

Jedna z najprostszych metod, zwana inwersją mocy (z ang. PI - Power Inversion), bazuje na tym, że zakłócenie docierające do anteny jest znacznie silniejsze niż pożądany sygnał. Zatem szyk należy sfazować w taki sposób, aby wypadkowy zysk na danym kierunku był odwrotnie proporcjonalny do mocy sygnału, który z tego kierunku dociera. Układ eliminacji spoofingu, bazujący na algorytmie odwrócenia mocy, został opisany w [19].

Znając postać sygnału użytecznego po stronie odbiorczej, można zastosować metodę minimalizacji błędu średniokwadratowego MMSE. Polega ona na takim wysterowaniu szyku, aby uzyskać jak najmniejszą różnicę pomiędzy sygnałem wyjściowym a, wytwarzaną lokalnie, repliką sygnału użytecznego.

Inną, jedną z najbardziej powszechnych, metodą fazowania szyku jest formowanie wiązki (z ang. beamforming). Polega ono na skierowaniu wiązki głównej charakterystyki kierunkowej na źródło sygnału użytecznego. W przypadku, gdy nie występują zakłócenia kierunkowe, a szumy w torach odbiorczych są wzajemnie nieskorelowane, formowanie wiązki umożliwia nawet M-krotną poprawę stosunku SNR sygnału użytecznego w stosunku do odbioru jednoantenowego, gdzie M jest liczbą elementów antenowych szyku. Oczywiście wymogiem zastosowania tej metody jest znajomość kierunku nadejścia sygnału użytecznego lub - równoważnie - znajomość opóźnień fazowych tego sygnału pomiędzy elementami szyku. Przykłady zastosowania beamformingu do poprawy jakości odbioru sygnałów GNSS można znaleźć np. w [9, 18, 27, 28, 42, 49].

Analogicznie, znając kierunki nadejścia zakłóceń, można ustalić na nich zera (minima zysku) charakterystyki. Taka metoda jest określana mianem kształtowania zer lub sterowania zerami (ang. null-steering, zero-forcing) [32, 85, 94, 103].



Rysunek 2.3: Charakterystyka 4-elementowego układu antenowego z ustalonymi trzema zerami

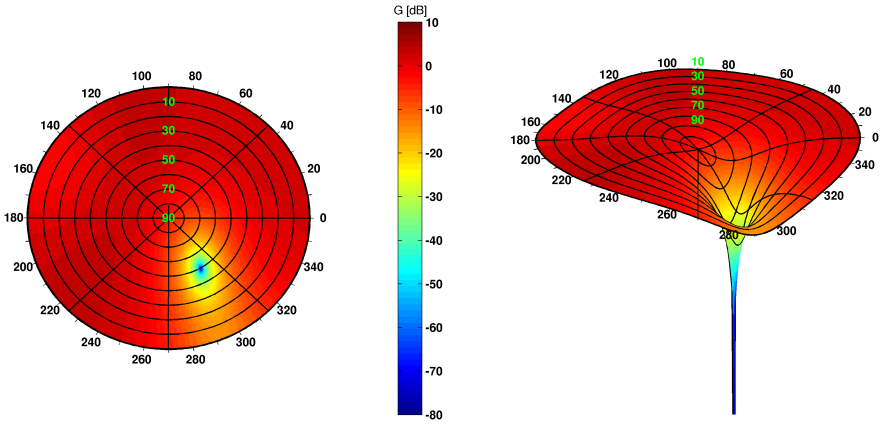
Zaproponowana w punkcie 2.3.1, metoda wykrywania spoofingu wiąże się z estymacją opóźnień fazowych sygnałów spoofera. Informacja o tych opóźnieniach może być również użyta w procedurze filtracji przestrzennej poprzez sterowanie zerem. Właśnie z uwagi na możliwość sprzęgnięcia tych metod wykrywania i eliminacji spoofingu, zdecydowano się na zastosowanie,

w analizowanym systemie antyspoofingowym, eliminacji spoofingu poprzez zastosowanie podejścia null-steering.

W metodzie sterowania zerami można ukształtować charakterystykę odbiorczą w taki sposób, aby występowało w niej maksymalnie M-1 zer, gdzie M jest liczbą elementów szyku. Jednakże należy się w takim przypadku liczyć ze stosunkowo silnym tłumieniem sygnałów docierających z innych kierunków niż sygnały niepożądane (Rys. 2.3). Natomiast, jeśli dominująca składowa sygnału niepożądanego dociera z jednego kierunku, postać wektora wagowego $\overrightarrow{\mathbf{w}}$ opisuje poniższy wzór:

$$\overrightarrow{\mathbf{w}} = \left[\begin{array}{cccc} \frac{1}{\sqrt{P_1}} & \frac{e^{-j\Delta\phi_{1,2}}}{\sqrt{P_2(M-1)}} & \cdots & \frac{e^{-j\Delta\phi_{1,M}}}{\sqrt{P_M(M-1)}} \end{array} \right], \tag{2.2}$$

gdzie P_m jest mocą sygnału zakłócającego na wejściu m-tego elementu antenowego. Taka postać wektora wagowego umożliwia uzyskanie optymalnego kształtu charakterystyki odbiorczej [54], co przedstawia poniższy rysunek.



Rysunek 2.4: Charakterystyka 4-elementowego układu antenowego z ustalonym jednym zerem

2.4 Kryteria oceny rozwiązań antyspoofingowych

Zarówno metody wykrywania, jak i metody ograniczania wpływu spoofingu na pracę odbiornika, można ocenić pod kątem stopnia złożoności ich implementacji praktycznej oraz efektywności, tak jak zostało to przedstawione w Tab. 2.1. Jednakże taki sposób oceny jest bardzo ogólny i najczęściej niewystarczający z punktu widzenia odbiorcy/użytkownika oferowanego systemu. Konieczne jest, w takim przypadku, dokonanie bardziej wymiernej ewaluacji, w postaci wartości parametrów wyrażonych liczbowo. Z uwagi na bardzo specyficzny i nowatorski charakter tego typu rozwiązań, nie został dotychczas ustalony żaden standardowy zestaw takich parametrów oceny. W związku z tym, zostały one zdefiniowane w niniejszej rozprawie. Parametry te mają uniwersalny charakter, co oznacza, że nie służą wyłącznie do oceny efektywności konkretnego systemu analizowanego w tej pracy, lecz również mogą zostać użyte do porównania innych rozwiązań antyspoofingowych.

Autor rozprawy proponuje następujące podejście do zagadnienia oceny efektywności spoofingu. Mianowicie, wykrywanie spoofingu można ocenić poprzez analogię do parametrów używanych w radiolokacji, przy czym detekcji podlega sygnał spoofera, a nie, jak w przypadku radaru, impuls odbity od obiektu. Podstawowymi terminami teorii radiolokacji są prawdopodobieństwo detekcji P_D oraz prawdopodobieństwo fałszywego alarmu P_{FA}. Pierwsze mówi o tym, w jak dużej części przypadków zostanie prawidłowo wykryty spoofing i jest pożądane, aby było możliwie największe. Z kolei drugie opisuje jak często system zasygnalizuje wykrycie spoofingu, podczas gdy w rzeczywistości ten atak nie będzie realizowany, zatem powinno być jak najmniejsze. Wartości obu tych prawdopodobieństw zależą m.in. od ustalonego progu detekcji. Przy doborze wartości progowej jest konieczne zachowanie kompromisu pomiędzy P_D i P_{FA}. W zależności od pożądanych właściwości, można przyjąć dolną granicę akceptowalnego P_D, lub ograniczyć P_{FA} od góry. Oprócz progu, na prawdopodobieństwo detekcji mają wpływ czynniki uzależnione od wybranej metody wykrywania. W przypadku przyjętej tu metody porównywania opóźnień fazowych, zwiększenie błędu estymacji tych opóźnień, spowodowane m.in. spadkiem stosunku SNR sygnału spoofera, zmniejsza szanse poprawnego wykrycia ataku.

Oceniając efektywność metod eliminacji spoofingu, należy przede wszystkim określić w jakim stopniu ta eliminacja wpływa na liczbę prawdziwych i fałszywych sygnałów oraz ich wartości $\frac{C}{N_0}$. Metody eliminacji spoofingu oparte o przetwarzanie odbieranych sygnałów GPS, powinny charakteryzować się dwoma cechami. Po pierwsze, silnie tłumić sygnały pochodzące od spoofera lub oddzielać je od sygnałów użytecznych. Po drugie umożliwiać poprawne funkcjonowanie odbiornika GPS i zapewniać dostępność usługi lokalizacyjnej w oparciu o przetworzony sygnał. W przypadku metody sterowania zerami, tłumienie sygnału niepożądanego zależy od kierunku nadejścia sygnału oraz od błędu estymacji tego kierunku, który to błąd jest funkcją m.in. stosunku $\frac{C}{N_0}$ tego sygnału. Z kolei miarą dostępności usługi lokalizacyjnej jest prawdopodobieństwo widoczności określonej liczby satelitów. Można je określić statystycznie jako procent czasu, w jakim odbiornik, realizujący procedury antyspoofingowe, jest w stanie odbierać daną liczbę prawdziwych sygnałów GPS, zakładając brak przeszkód na trasach propagacji pomiędzy satelitami a anteną odbiornika.

Rozdział 3

Koncepcja budowy i działania systemu antyspoofingowego

W niniejszym rozdziale autor przedstawia własną koncepcję systemu przeciwdziałania spoofingowi GPS, działającego w oparciu o, wymienione w poprzednim rozdziale, wybrane metody przestrzennego przetwarzania odbieranych sygnałów.

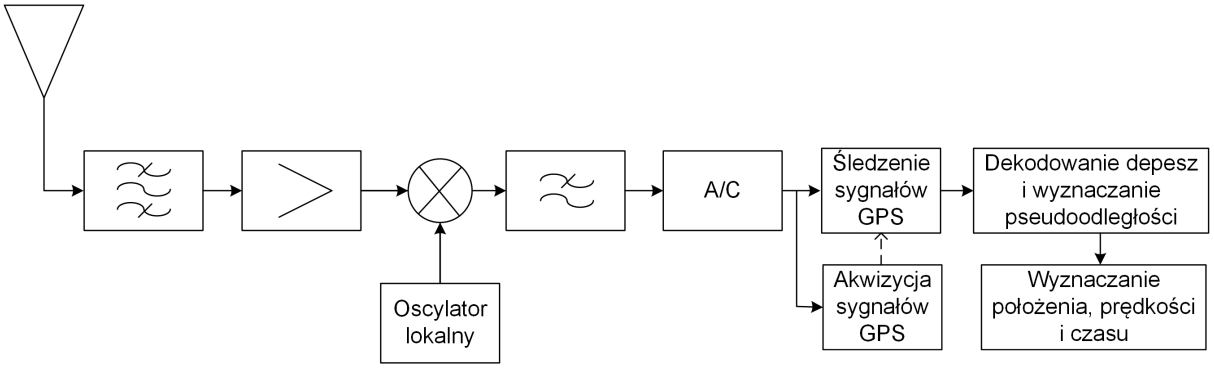
Pierwszą część rozdziału poświecono opisowi funkcjonowania odbiornika GPS, wyposażonego w proponowane rozwiązania ochrony przed spoofingiem. Punktem wyjścia dla tego opisu jest schemat i zasada działania konwencjonalnego odbiornika GPS. Następnie są omówione modyfikacje tego schematu, związane wymogami dotyczącymi integracji odbiornika z analizowanym systemem antyspoofingowym.

Pozostała część rozdziału została stanowi objaśnienie algorytmów przetwarzania sygnałów GPS, związanych z rozpatrywanymi metodami wykrywania i eliminacji spoofingu. W opisie uwzględniono zarówno algorytmy specyficzne dla przyjętych metod antyspoofingowych, jak również, wymagane do działania tych metod, algorytmy stosowane w standardowych odbiornikach GPS.

3.1 Schemat przetwarzania w odbiorniku antyspoofingowym

System antyspoofingowy, w proponowanej postaci, składa się z modułów funkcjonalnych, które stanowią rozszerzenie modelu działania standardowego odbiornika GPS. Aby pojąć sposób funkcjonowania odbiornika wyposażonego w mechanizmy ochrony przed spoofingiem, należy wpierw poznać zasadę działania odbiornika nie oferującego takiej ochrony.

W standardowym odbiorniku GPS, którego schemat przedstawia Rys. 3.1, sygnały odbierane przez antenę podlegają filtracji pasmowo przepustowej i są wzmacniane. Najczęściej odbywa się to już w samej antenie aktywnej, wyposażonej we wzmacniacz niskoszumowy i filtry wyodrębniające pasmo transmisji sygnałów jednego lub kilku systemów GNSS. W następnej kolejności, sygnał jest sprowadzany do pasma pośredniej częstotliwości lub do pasma podstawowego, poprzez mieszanie go z sygnałem wyjściowym oscylatora lokalnego. Wynikowy sygnał, poddany filtracji dolnoprzepustowej, może być następnie dalej przetwarzany w formie analogowej, albo zamieniony na postać cyfrową.



Rysunek 3.1: Schemat blokowy odbiornika GPS

Określenie pozycji odbiornika wymaga znajomości pseudoodległości od poszczególnych satelitów. Wymagane są także, przesyłane w formie depeszy nawigacyjnej, wartości parametrów opisujących ruch tych satelitów po ich orbitach. Aby odtworzyć dane nawigacyjne zawarte w sygnale danego satelity, jest konieczne skupienie widma sygnału, co uzyskuje się poprzez mnożenie sygnału wejściowego przez lokalną replikę. Replika to iloczyn przebiegu ciągu pseudolosowego

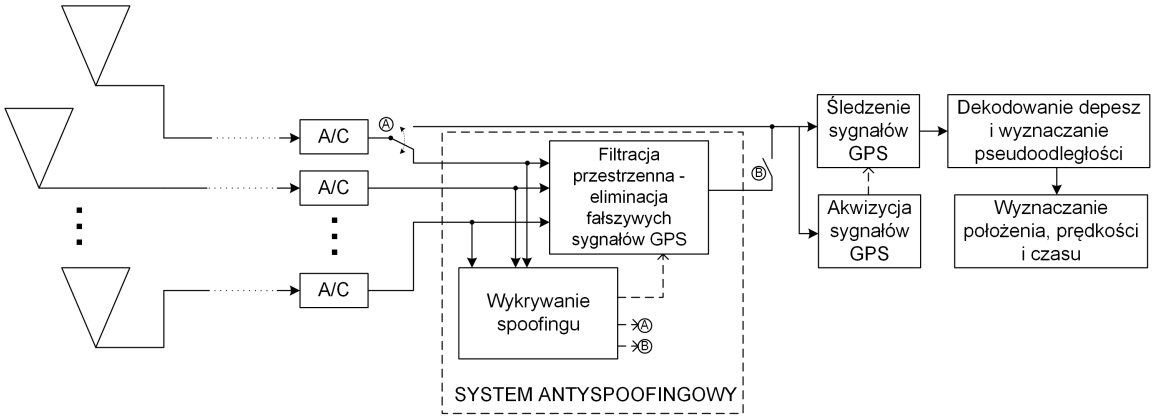
C/A i fali harmonicznej o częstotliwości możliwie bliskiej częstotliwości środkowej odbieranego sygnału GPS. Aby wytworzyć replikę odpowiednio zsynchronizowaną z sygnałem pochodzącym z satelity, jest konieczne wyznaczenie parametrów tego sygnału, co jest realizowane na kolejnych etapach przetwarzania.

W systemach GNSS jest stosowana technika transmisji zwana bezpośrednim rozpraszaniem widma - DSSS. Odbiór tego typu sygnałów jest realizowany dwuetapowo. Można wyróżnić tzw. fazę akwizycji i, następującą po niej, fazę śledzenia [8]. Pierwsza z nich polega na określeniu, które sygnały, spośród wszystkich sygnałów nadawanych w danym systemie, aktualnie docierają do odbiornika. W przypadku systemu GPS sygnały są rozróżniane w oparciu o postaci ich ciągów rozpraszających C/A (technika DS-CDMA). Z kolei w systemie GLONASS zastosowano wielodostęp z podziałem częstotliwości - FDMA[1] [55]. Poza samą identyfikacją sygnałów, w bloku akwizycji są określane odchyłki dopplerowskie częstotliwości nośnej sygnałów oraz względne przesunięcia czasowe ciągów rozpraszających C/A. Są to parametry które umożliwiają wytworzenie replik sygnałów. W związku ze zmiennością wartości tych parametrów w czasie, jest wymagana nieustanna ich aktualizacja w odbiorniku. To właśnie blok śledzenia realizuje równoczesną aktualizację częstotliwości Dopplera i fazy ciągu C/A. Sygnały są w tym miejscu mnożone przez swoje repliki oraz są wykrywane przeskoki fazy fali nośnej o $\pm\pi$, związane ze zmianą znaku bitu depeszy. Można zatem powiedzieć, że skupianie widma sygnału odbywa się w fazie śledzenia. Różnice pseudoodległości od poszczególnych satelitów mogą być ustalone w oparciu o wykrycie chwil zmian znaku bitu, wyznaczających początek ramki depeszy nawigacyjnej. Parametry orbitalne satelitów i informacje o pseudoodległościach są przekazywane do bloku obliczającego pozycję i prędkość odbiornika oraz aktualny czas systemowy. Wyznaczone parametry nawigacyjne stanowią informację dla bloku prezentacji, który może je wyświetlić np. w postaci tekstowej lub obiektu graficznego naniesionego na podkład mapowy.

Sposób realizacji systemu antyspoofingowego w postaci proponowanej przez doktoranta, wymaga użycia, zamiast pojedynczej anteny, szyku antenowego (Rys. 3.2). Sygnał z wyjścia każdej anteny odbiorczej podlega filtracji częstotliwościowej, wzmocnieniu i przemianie częstotli-

[1] W zmodernizowanych sygnałach GLONASS również jest stosowane CDMA

wości, tak jak jest to realizowane w standardowym odbiorniku GPS. Przetworzone w ten sposób sygnały są podane na wejście bloków wykrywania spoofingu i filtracji przestrzennej. Procedura wykrywania określa, czy spoofing jest aktywny, a jeśli tak, to które sygnały są fałszywe i jakie są ich opóźnienia fazowe mierzone pomiędzy elementami szyku antenowego. Informacja o obecności spoofingu może być użyta do sterowania położeniem przełączników Ⓐ i Ⓑ. W zależności od ich konfiguracji, odbiornik GPS pracuje w trybie standardowym albo w trybie antyspoofingowym.



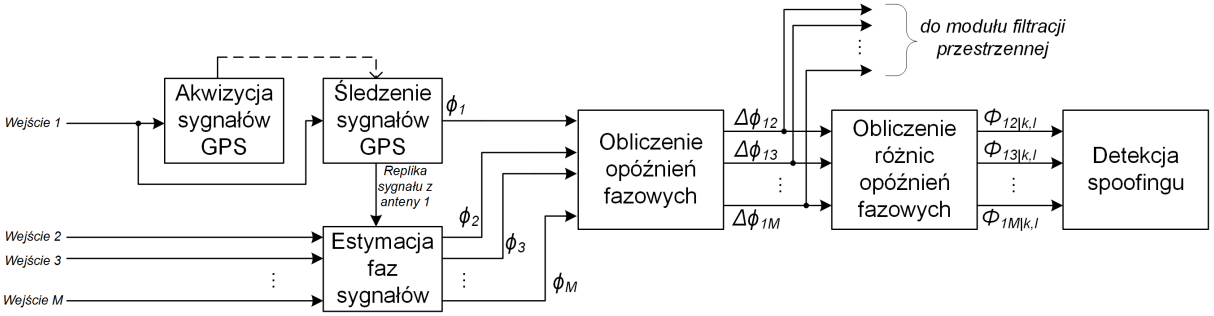
Rysunek 3.2: Schemat blokowy odbiornika GPS z systemem antyspoofingowym

Wyznaczone opóźnienia fazowe, jak również moce sygnałów z poszczególnych anten, są przekazywane do bloku filtracji przestrzennej, który wyznacza postać wektora wagowego, zgodnie z formułą (2.2). Filtracja przestrzenna jest realizowana poprzez mnożenie wektorów próbek sygnałów, odbieranych przez różne anteny, z wektorem wagowym. Proces filtracji opisuje poniższy wzór:

$$s_{fp}[t_n] = \mathbf{s}[t_n] \cdot \mathbf{w}^T[t_n] = \\ = \begin{bmatrix} s_1[t_n] & s_2[t_n] & \dots & s_M[t_n] \end{bmatrix} \cdot \begin{bmatrix} w_1[t_n] & w_2[t_n] & \dots & w_M[t_n] \end{bmatrix}^T, \quad (3.1)$$

gdzie $s_{fp}[t_n]$ to wartość próbki sygnału po filtracji przestrzennej, $s_m[t_n]$ to wartość próbki sygnału z wyjścia m-tego elementu antenowego, $w_m[t_n]$ to aktualna wartość m-tego współczynnika wagowego, a ^{T} oznacza transpozycję. Jeśli system antyspoofingowy stanowi integralną część odbiornika GPS, tak jak to przedstawiono na Rys. 3.2, sygnał z wyjścia bloku filtracji przestrzennej

jest bezpośrednio przekazywany do bloków akwizycji i śledzenia sygnałów. Możliwa jest również realizacja systemu antyspoofingowego jako niezależnego układu. W takim przypadku, sygnał wyjściowy filtru przestrzennego jest zamieniany z powrotem na postać analogową i przenoszony do pasma częstotliwości L1. W takiej formie może być on podany na wejście w.cz. (wejście anteny zewnętrznej) dowolnego odbiornika GPS.



Rysunek 3.3: Schemat bloku wykrywania spoofingu

Budowa bloku wykrywania spoofingu, który stanowi pierwszy moduł systemu antyspoofingowego, została przedstawiona na Rys. 3.3. W pierwszej kolejności realizuje on etap akwizycji sygnałów GPS, który jest realizowany w taki sam sposób jak w standardowym odbiorniku. Akwizycja odbywa się w oparciu o sygnał z wyjścia tylko jednego elementu szyku antenowego. W dalszej części tej pracy przyjęto, że jest to pierwszy element antenowy, którego środek fazy stanowi punkt referencyjny dla pomiarów opóźnień fazowych sygnałów docierających do innych elementów. Blok śledzenia sygnałów w systemie antyspoofingowym również wykazuje duże podobieństwo do swojego odpowiednika w standardowym odbiorniku. Pełna procedura śledzenia jest realizowana tylko dla sygnału odbieranego przez pierwszy element antenowy. Jednakże, przez odtworzoną replikę tego sygnału jest mnożony nie tylko on sam, ale także sygnały z wyjść pozostałych elementów szyku. Umożliwia to wyznaczenie faz fal nośnych wszystkich sygnałów odbieranych przez wszystkie elementy antenowe, a w konsekwencji ich opóźnień fazowych i różnic tych opóźnień pomiędzy sygnałami modulowanymi różnymi ciągami C/A. Różnice opóźnień fazowych stanowią informację wejściową dla właściwego algorytmu detekcji spoofingu.

Decyzja o wykryciu spoofingu jest podejmowana w oparciu o porównanie różnic opóźnień

fazowych z wartością progową, uzależnioną od liczby odbieranych sygnałów i ich jakości. Wystąpienie spoofingu jest stwierdzane gdy zmierzone różnice opóźnień fazowych pochodzące od co najmniej czterech satelitów są mniejsze niż ustalony próg. Największa liczba satelitów, dla której kryterium detekcji jest spełnione, jest uznawana za liczbę fałszywych sygnałów nadawanych przez spoofer. Opóźnienia fazowe, pochodzące od sygnałów uznanych za fałszywe, są uśredniane i przekazywane do bloku filtracji przestrzennej.

3.2 Algorytmy przetwarzania sygnałów GPS

Na efektywność działania rozpatrywanego systemu antyspoofingowego duży wpływ ma dokładność wyznaczania opóźnień fazowych sygnałów, na co z kolei wpływa m.in. sposób realizacji funkcji akwizycji i śledzenia sygnałów GPS. Dlatego też, w dalszej części tego rozdziału, zostały dokładnie opisane algorytmy tych operacji, które zostały zastosowane przy realizacji badań symulacyjnych i pomiarowych, którym zostały poświęcone dalsze rozdziały niniejszej pracy. Zaprezentowane poniżej metody softwarowej realizacji procedur akwizycji i śledzenia sygnałów GPS, zostały w dużej mierze oparte o algorytmy opisane w [7].

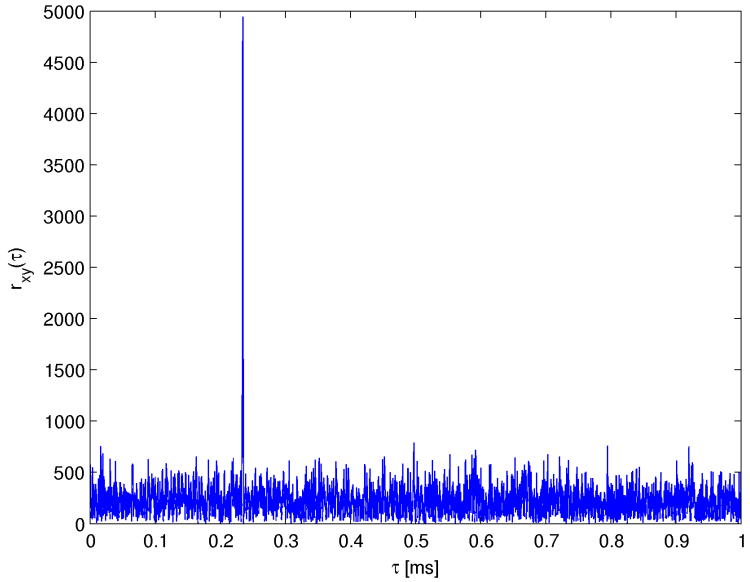
Ponadto, w niniejszym punkcie rozprawy przedstawiono, w jaki sposób sposób, są obliczane opóźnienia fazowe fal nośnych sygnałów i różnice tych opóźnień. Zdefiniowano również postać wyrażenia logicznego, na podstawie którego jest podejmowana decyzja o wykryciu spoofingu.

Na zakończenie scharakteryzowano wybrane algorytmy wyznaczania parametru $\frac{C}{N_0}$, określającego jakość odbieranych sygnałów. Prawidłowe obliczanie wartości tego parametru jest niezwykle istotne z punktu widzenia ustalania progu detekcji spoofingu, a także całościowej oceny efektywności rozwiązań antyspoofingowych.

3.2.1 Akwizycja sygnałów GPS

Aby określić numery satelitów GPS, których sygnały są odbierane w danej chwili, odbiornik oblicza postać funkcji korelacji skrośnej sygnału odbieranego z lokalną repliką tego sygnału. Replika ta stanowi iloczyn fali nośnej i przebiegu prostokątnego, odpowiadającego ciągowi

pseudolosowemu C/A, przypisanemu do konkretnego satelity. W przypadku obecności sygnału o odpowiednio wysokim stosunku sygnał-szum, maksimum funkcji korelacji jest znacznie większe od pozostałych prążków. Przykładowy przebieg funkcji korelacji, w przypadku odbioru sygnału o $\frac{C}{N_0}$ równym 50 dBHz (SNR = -13 dB), został przedstawiony na Rys. 3.4. Widać na nim wyraźne maksimum, które występuje dla argumentu τ równego ok. 230 μs. Oznacza to, że właśnie tyle wynosi przesunięcie czasowe chwili rozpoczęcia ciągu C/A od początku analizowanego segmentu sygnału GPS.



Rysunek 3.4: Przebieg funkcji korelacji sygnału GPS o $\frac{C}{N_0} = 50\ dBHz$

Funkcja korelacji może być obliczana w dziedzinie czasu dla sygnałów dyskretnych według następującego wzoru:

$$r_{xy}[\tau_n] = \sum_{t_n=-\infty}^{\infty} x^*[t_n] \cdot y[t_n + \tau_n], \tag{3.2}$$

gdzie $x[t_n]$ reprezentuje próbki sygnału odbieranego, $y[t_n]$ reprezentuje próbki repliki tego sygnału, τ_n jest, wyrażonym liczbą próbek, względnym opóźnieniem sygnału w stosunku do repliki, a * oznacza sprzężenie zespolone. Z punktu widzenia złożoności obliczeniowej korzystniejsze jest

wyznaczanie funkcji korelacji w dziedzinie częstotliwości według poniższego wzoru:

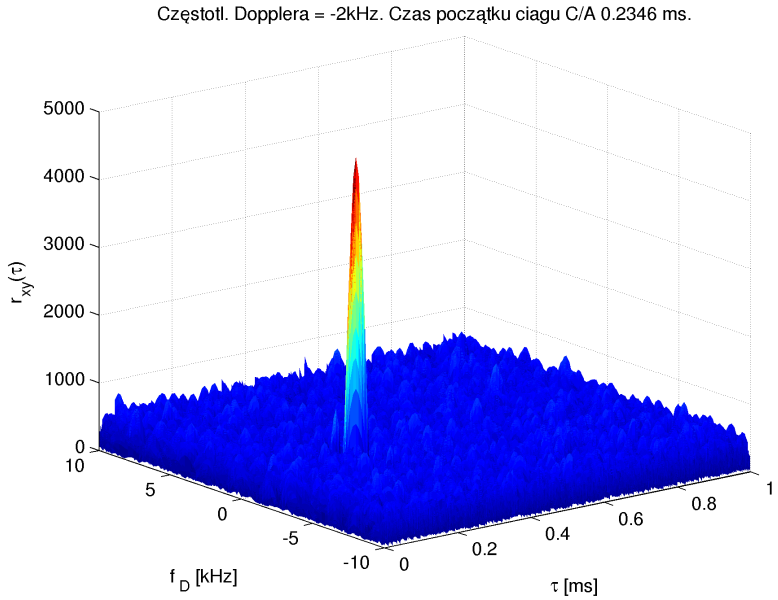
$$r_{xy}[\tau_n] = IFFT\left\{FFT\left\{x[t_n]\right\} \cdot FFT\left\{y[t_n]\right\}^*\right\}, \tag{3.3}$$

w którym FFT oznacza prostą szybką transformację Fouriera, a $IFFT$ - odwrotną szybką transformację Fouriera.

W odbiorniku GPS funkcję korelacji oblicza się najczęściej w oparciu o segment sygnału o długości 1 ms. Wynika to stąd, że właśnie tak długi jest okres powtarzania ciągu pseudolosowego C/A. Położenie maksimum funkcji korelacji wskazuje numer pierwszej próbki kolejnej realizacji tego ciągu. W przypadku słabych sygnałów GPS ($\frac{C}{N_0} < 40$ dBHz) wartość pierwszej próbki ciągu jest porównywalna z wartościami innych próbek funkcji korelacji, co utrudnia wykrycie takiego sygnału. Ponadto, wartość tej próbki jest mniejsza w przypadku wystąpienia zmiany znaku bitu depeszy nawigacyjnej w czasie trwania 1 ms. Poprawę widoczności maksimum w takich sytuacjach można uzyskać m.in. poprzez uśrednianie funkcji korelacji, obliczonych na podstawie kilku kolejnych, jednomilisekundowych segmentów sygnału odbieranego. Położenie początku ciągu jest jednym z parametrów wymaganych do rozpoczęcia fazy śledzenia sygnału. Drugim jest częstotliwość Dopplera. Biorąc pod uwagę ruch satelitów względem odbiornika, jak również ruch samego odbiornika względem Ziemi, stwierdzono, że zakres możliwych odchyłek dopplerowskich sygnału GPS obejmuje pasmo ±10 kHz względem częstotliwości nośnej L1[2]. Zgrubne określenie częstotliwości Dopplera wymaga przeszukania tego pasma z określoną rozdzielczością. Przyjmuje się, że krok zmiany częstotliwości nie powinien być większy niż odwrotność czasu trwania przetwarzanego segmentu sygnału. W przypadku 1 ms sygnału, rozdzielczość zgrubnej estymacji odchyłki dopplerowskiej wynosi 1 kHz. Zatem, jeśli zakres możliwych przesunięć Dopplera ma szerokość 20 kHz, należy obliczyć 21 postaci funkcji korelacji dla replik sygnału o różnych częstotliwościach nośnych. Zgrubną odchyłką dopplerowską jest ta, dla której występuje największa korelacja. Przykładowy wynik obliczeń funkcji korelacji, w dziedzinie czas/częstotliwość, został przedstawiony na Rys. 3.5. Dalsze zwiększanie rozdzielczości częstotliwościowej, poprzez obli-

[2]Zakres ten obejmuje nawet odbiorniki w samolotach poruszających się z prędkością ponaddźwiękową. W przypadku odbiorników stacjonarnych, lub wolno poruszających się, można ograniczyć go do ±5 kHz

czanie np. 41 wariantów funkcji korelacji, nie jest wskazane, gdyż powoduje istotny wzrost liczby obliczeń, co ma duże znaczenie w przypadku odbiorników działających w czasie rzeczywistym.



Rysunek 3.5: Funkcja korelacji w dziedzinie czas/częstotliwość

Dokładność estymacji częstotliwości Dopplera co do 1 kHz nie jest wystarczająca dla poprawnej realizacji etapu śledzenia, gdzie filtr pętli ma pasmo rzędu kilku lub kilkunastu Hz. Bardziej precyzyjnej estymacji można dokonać w oparciu o wartości względnych przesunięć fazowych pomiędzy kilkoma kolejnymi segmentami sygnału o długości 1 ms. Niech $X[k]$ będzie dyskretną transformatą Fouriera (DFT) segmentu sygnału $x[t_n]$, obliczoną dla k-tego prążka widma, odpowiadającego częstotliwości $f_{D,zgr}$ wyznaczonej w sposób zgrubny:

$$X[k] = \sum_{t_n=0}^{T_{n,1ms}-1} x[t_n] \cdot e^{-i\frac{2\pi k t_n}{T_{n,1ms}}}, \tag{3.4}$$

gdzie $T_{n,1ms}$ jest liczbą próbek sygnału w czasie trwania 1 ms. Wtedy, fazę początkową l-tego segmentu sygnału można wyznaczyć, korzystając ze wzoru:

$$\phi[l \cdot T_{n,1ms}] = arctg\left(\frac{Im\{X[k]\}}{Re\{X[k]\}}\right) \qquad l = 0, 1, 2, \ldots. \tag{3.5}$$

Znając fazy poczatkowe dwóch kolejnych segmentów, można wyznaczyć poprawkę częstotliwości wg poniższego wzoru:

$$\Delta f_D[l \cdot T_{n,1ms}] = \frac{\phi[l \cdot T_{n,1ms}] - \phi[(l-1) \cdot T_{n,1ms}]}{2\pi \cdot 1ms} \qquad l = 1, 2, 3, \ldots. \tag{3.6}$$

Ostatecznie, dokładna wartość częstotliwości Dopplera f_D jest obliczona jako:

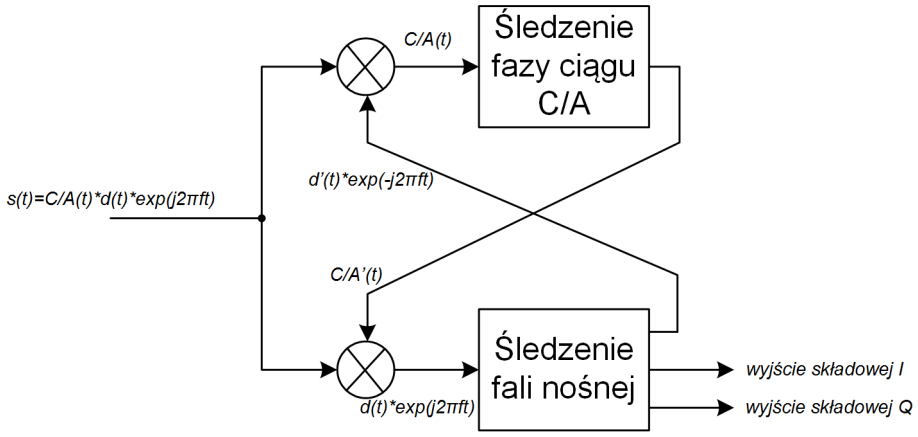
$$f_D[l \cdot T_{n,1ms}] = f_{D,zgr} + \Delta f_D[l \cdot T_{n,1ms}] \qquad l = 1, 2, 3, \ldots. \tag{3.7}$$

Aby zminimalizować wpływ szumu należy obliczyć poprawki częstotliwości dla kilku, np. pięciu, segmentów sygnału i uśrednić uzyskane wyniki. Ponadto, w obecności szumu może wystąpić niejednoznaczność fazy, prowadząca do nieprawidłowego wyznaczenia poprawki odchyłki dopplerowskiej Δf_D. Dlatego też, przed obliczeniem Δf_D, aby wyeliminować tę niejednoznaczność, należy dodatkowo obliczyć funkcję korelacji dla częstotliwości oddalonych o ± 400 Hz względem $f_{D,zgr}$. Jeśli dla którejś z tych dwóch częstotliwości prążek funkcji autokorelacji będzie wyższy niż dotychczasowy, zostaje ona wybrana jako nowa wartość $f_{D,zgr}$.

Przy wyznaczaniu różnic faz początkowych należy także wykrywać i korygować przeskoki fazy spowodowane zmianami znaku bitów depeszy nawigacyjnej. W przeciwnym wypadku wartość Δf_D będzie obliczona błędnie. Przyjmuje się, że wartość bezwzględna różnicy faz pomiędzy kolejnymi segmentami nie powinna przekroczyć $2\pi/5$, przy założeniu, że różnica faz jest odwzorowana w przedziale od 0 do 2π. Jeśli fazy różnią się bardziej, oznacza to, że wystąpił przeskok spowodowany zmianą bitu, który należy skorygować poprzez dodanie lub odjęcie π.

3.2.2 Śledzenie sygnałów GPS

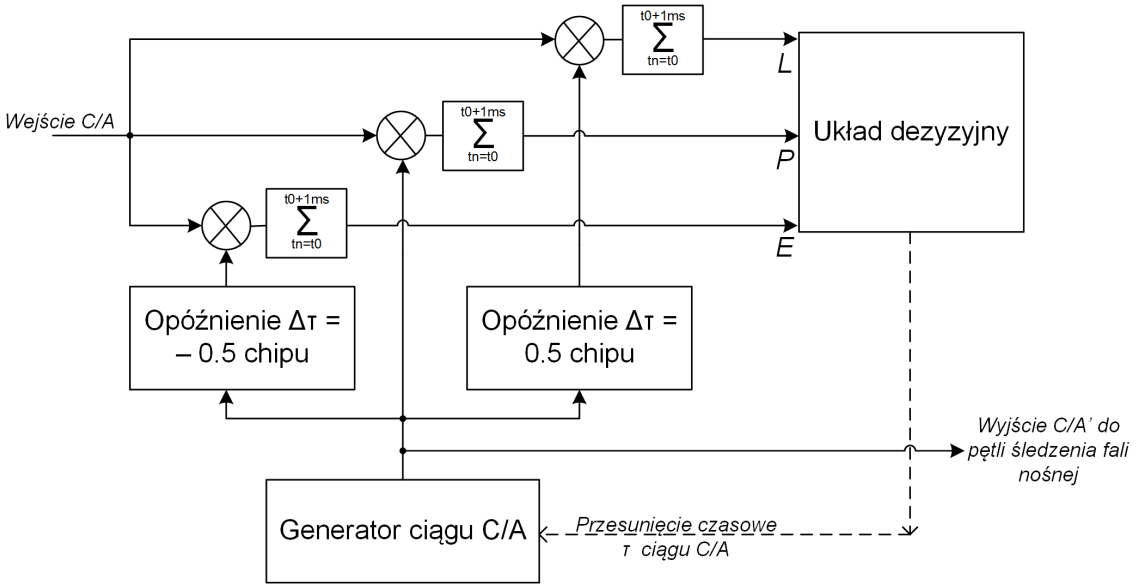
Etap śledzenia sygnału GPS można rozpocząć, dysponując następującym zestawem informacji o tym sygnale: numerem ciągu pseudolosowego C/A, położeniem początku tego ciągu w obrębie 1 ms sygnału oraz częstotliwością Dopplera. W bloku śledzenia działają dwie, wzajemnie sprzężone pętle: pętla śledzenia fali nośnej oraz pętla śledzenia fazy ciągu pseudolosowego. Schemat ich współpracy został przedstawiony na poniższym rysunku:



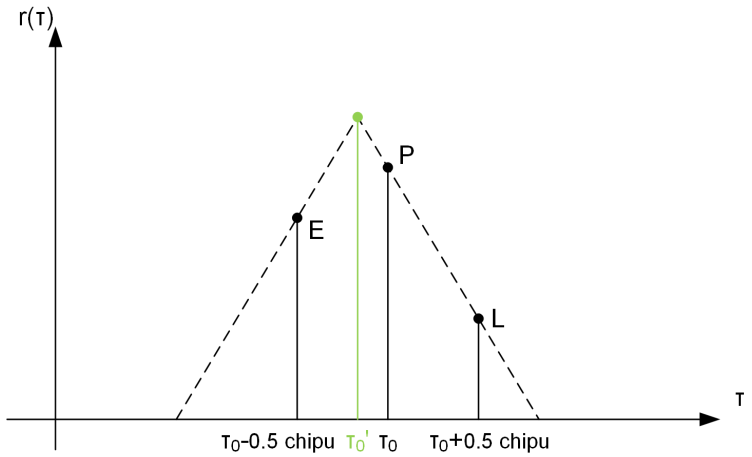
Rysunek 3.6: Schemat układu śledzenia sygnału GPS

Pętla śledzenia fazy ciągu pseudolosowego (Rys. 3.7) operuje na sygnale pomnożonym przez lokalną replikę zespolonej fali nośnej, z uwzględnieniem odchyłki dopplerowskiej. Częstotliwość środkowa tak przetworzonego sygnału jest równa lub bliska 0 Hz. Śledzenie fazy ciągu pseudolosowego polega na aktualizacji położenia maksimum funkcji korelacji, które, w zależności od znaku częstotliwości Dopplera, będzie się przesuwało w prawo lub w lewo. Aby określić zmianę położenia najwyższego prążka, są konieczne co najmniej trzy korelatory. Każdy z nich oblicza wartość funkcji korelacji dla innego przesunięcia ciągu C/A. Korelator P (z ang. prompt) oblicza wartość funkcji korelacji dla bieżącej fazy ciągu, z kolei korelatory E i L (z ang. early i late) stosują postaci ciągu przyspieszone i opóźnione względem korelatora P. Względne przesunięcia czasowe ciągu pomiędzy kolejnymi korelatorami wynoszą zazwyczaj połowę czasu trwania elementarnego symbolu ciągu C/A (tzw. chipu), równą ok. 0,5 μs.

Funkcja korelacji ma kształt trójkąta w przedziale ± 1 chip wokół maksimum. Fazy ciągów w korelatorach E, P i L muszą być dobrane tak, aby wszystkie znajdowały się w obrębie tego trójkąta (Rys. 3.8). Jeśli wartości na którymś z wyjść korelatorów E lub L przewyższają wyjście korelatora P, faza lokalnie wytwarzanego ciągu zostaje zaktualizowana. Aby poprawić dokładność wyznaczania przesunięcia ciągu C/A, można zastosować większą liczbę korelatorów E i L, o różnych przesunięciach czasowych.



Rysunek 3.7: Schemat blokowy pętli śledzenia fazy ciągu pseudolosowego C/A



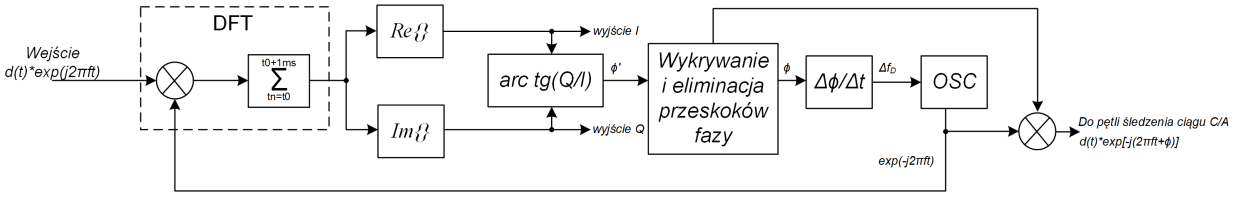
Rysunek 3.8: Wartości wyjściowe korelatorów E, P i L w na tle funkcji autokorelacji ciągu C/A

Sygnałem wejściowym dla pętli śledzenia fali nośnej (Rys. 3.9) jest sygnał o skupionym widmie, powstały na skutek pomnożenia odbieranego sygnału GPS przez lokalnie wytworzony, zsynchronizowany z sygnałem, ciąg pseudolosowy (taki sam jak w korelatorze P). Pętla na bieżąco estymuje częstotliwość Dopplera, podobnie do tego, jak jest to wykonywane na etapie

akwizycji. W tym wypadku jednak, rozdzielczość częstotliwości musi być większa niż odległość pomiędzy prążkami FFT, wynosząca 1 kHz. Fazy początkowe mogą być wyznaczane w oparciu o transformaty DFT obliczane dla niecałkowitych wartości k. Takie rozwiązanie wiąże się z problemem nieciągłości funkcji bazowych DFT na granicach kolejnych segmentów sygnału, co wymaga dodawania odpowiednich poprawek $\delta\phi$ do tak wyznaczonych faz początkowych ϕ :

$$\delta\phi[l \cdot T_{n,1ms}] = 2\pi(k \mod 1) + (\delta\phi[(l-1) \cdot T_{n,1ms}] \mod 2\pi) \qquad l = 1, 2, 3, \ldots, \tag{3.8}$$

gdzie operator mod oznacza resztę z dzielenia liczb rzeczywistych, zaś $k = \frac{f_D}{1kHz}$, a $\delta\phi[0] = 0$.



Rysunek 3.9: Schemat blokowy pętli śledzenia fali nośnej

3.2.3 Wyznaczanie opóźnień fazowych i ich różnic

W proponowanym systemie antyspoofingowym jest konieczne wyznaczenie faz wszystkich sygnałów z wyjść elementów szyku antenowego. Faza sygnału z pierwszego elementu jest obliczana przy użyciu wyrażeń (3.4) i (3.5), równocześnie z estymacją częstotliwości sygnału. Fazy sygnałów z pozostałych $M-1$ anten mogą być wyznaczone w sposób analogiczny, tzn.:

$$\phi_m[l \cdot T_{n,1ms}]|_{m=2\ldots M} = arctg\left(\frac{Im\{X_m[k]\}}{Re\{X_m[k]\}}\right)) \qquad l = 1, 2, 3, \ldots, \tag{3.9}$$

gdzie $X_m[k]$ oznacza transformatę DFT sygnału z wyjścia m-tego elementu antenowego. W oparciu o tak wyznaczone fazy można wyznaczyć opóźnienia fazowe $\Delta\phi$ sygnału s_i, mierzone pomiędzy pierwszym elementem szyku a pozostałymi:

$$\Delta\phi_{1,m|s_i}|_{m=2\ldots M} = \phi_1 - \phi_m. \tag{3.10}$$

Do wykrycia spoofingu używane są wartości różnic Φ opóźnień fazowych pomiędzy sygnałami GPS modulowanymi różnymi ciągami C/A:

$$\Phi_{1,m|s_i,s_j} = \Delta\phi_{1,m|s_i} - \Delta\phi_{1,m|s_j}. \tag{3.11}$$

Spoofing jest wykryty, gdy wartości bezwzględne różnic opóźnień fazowych, dla co najmniej czterech sygnałów o różnych ciągach C/A, są mniejsze niż wartość progowa, tzn spełnione jest następujące wyrażenie logiczne:

$$\bigvee_{\substack{S_{spoof}\subseteq S_{odb} \\ \overline{\overline{S}}_{spoof}\geqslant 4}} \bigwedge_{\substack{m=2...M \\ i,j\in S_{spoof} \\ i\neq j}} |\Phi_{1,m|s_i,s_j}| \leqslant \Phi_{prog}. \tag{3.12}$$

Wyrażenie to należy interpretować następująco: *Spoofing GPS jest obecny, gdy istnieje zbiór S_{spoof} o mocy nie mniejszej niż 4, stanowiący podzbiór zbioru S_{odb} wszystkich aktualnie odbieranych sygnałów GPS, taki, że dla każdej pary elementów antenowych $[1, m]$ i dla każdej pary sygnałów $[i, j]$, należących do zbioru S_{spoof}, wartość bezwzględna różnicy opóźnień fazowych nie przekracza wartości Φ_{prog}, zwanej progiem detekcji spoofingu.*

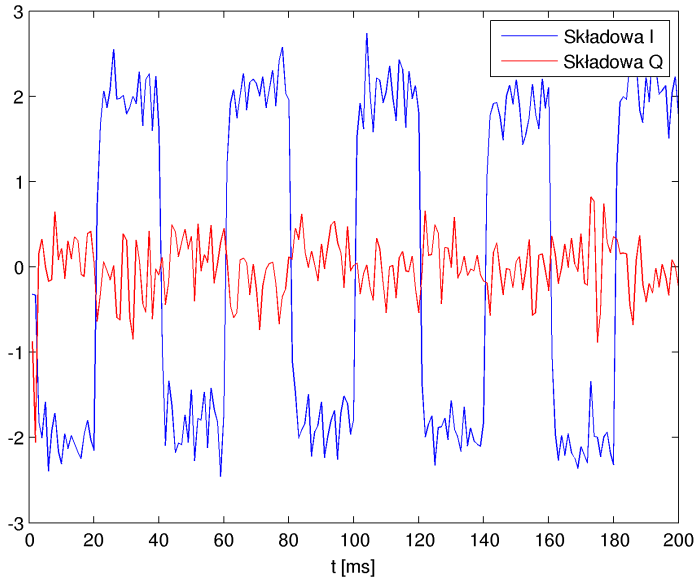
Sygnały ze zbioru S_{spoof} oznaczają te pochodzące od sygnałów spoofera. Pozostałe sygnały ze zbioru sygnałów odbieranych S_{odb} są albo prawdziwymi sygnałami z satelitów GPS, albo sygnałami spoofera, dla których Φ przekroczyło wartość progową wskutek błędu estymacji. Do obliczenia wektora wag filtracji przestrzennej należy użyć uśrednionych opóźnień fazowych $\Delta\phi_{1,i|s_i,s_j}$ sygnałów ze zbioru S_{spoof}.

3.2.4 Określanie wartości $\frac{C}{N_0}$ sygnałów GPS

Próg detekcji spoofingu jest uzależniony nie tylko od liczby odbieranych fałszywych sygnałów, ale także od jakości tych sygnałów. W przypadku systemów z widmem rozproszonym, miarą stosunku sygnał-szum jest $\frac{C}{N_0}$, czyli stosunek mocy fali nośnej do widmowej gęstości mocy szumu w pasmie użytecznym. Wartość $\frac{C}{N_0}$ jest obliczana niezależnie dla każdego satelity, na podstawie przebiegów składowych I i Q sygnału, wyznaczonych w trakcie fazy śledzenia. Przy-

kładowe przebiegi odtworzonych wartości I i Q wraz z odpowiadającym im przebiegiem zmian fazy, zostały przedstawione na Rys. 3.10 i 3.11.

Obliczenia $\frac{C}{N_0}$ muszą być dokonywane z użyciem wyłącznie takich fragmentów przebiegów I i Q, w których nie występuje zmiana bitu nawigacyjnego, tzn. takich, dla których chwilowe wartości modułu $|I + jQ|$ nie przebiegają w pobliżu 0. W przeciwnym wypadku wartość $\frac{C}{N_0}$ będzie zaniżona.

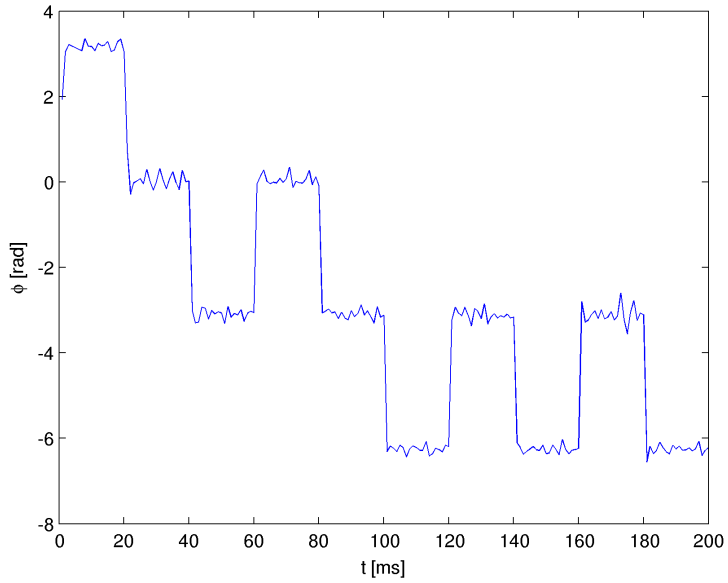


Rysunek 3.10: Przebieg składowych I i Q na wyjściu pętli śledzenia fali nośnej

W literaturze proponowanych jest wiele algorytmów obliczania $\frac{C}{N_0}$ w systemie GPS. Poniżej przybliżono trzy spośród nich: metodę sumowania wariancji, metodę Beaulieu oraz metodę momentów. Jedna z tych trzech metod zostanie zastosowana w realizowanym systemie antyspoofingowym. Jej wybór zostanie dokonany w oparciu o badania symulacyjne, opisane w kolejnym rozdziale.

W metodzie sumowania wariancji (z ang. Variance Summing Method) [86] najpierw jest obliczana suma kwadratów próbek przebiegów I i Q:

$$Z[l] = \left(I^2[l] + Q^2[l]\right). \tag{3.13}$$



Rysunek 3.11: Przebieg fazy fali nośnej modulowanej ciągiem danych nawigacyjnych

Następnie, jest wyznaczana średnia moc fali nośnej:

$$\left(\frac{NA}{2}\right)^2 = \sqrt{\overline{Z}^2 - \sigma_Z^2}, \tag{3.14}$$

gdzie $\overline{Z}$ jest wartością średnią Z, a σ_Z^2 jest wariancją Z. Z kolei wariancja składowej szumowej jest obliczana jako:

$$\sigma_{IQ}^2 = \frac{1}{2}\left(\overline{Z}^2 - \sqrt{\overline{Z}^2 - \sigma_Z^2}\right). \tag{3.15}$$

Ostatecznie, wartość $\frac{C}{N_0}$ można obliczyć zgodnie z poniższym wzorem:

$$\frac{C}{N_0} = 10\log_{10}\left[\frac{(NA/2)^2}{2T_{seg}\sigma_{IQ}^2}\right], \tag{3.16}$$

gdzie T_{seg} jest długością czasu całkowania w korelatorze, przy którym wyznaczono wartości składowych I i Q (tzw. czas akumulacji). Wynosi on 1 ms lub wielokrotność tej długości czasu.

Drugi z rozpatrywanych algorytmów - metoda Beaulieu [25, 26] bazuje jedynie na analizie przebiegu próbek składowej synfazowej I. Moc sygnału użytecznego jest tutaj wyznaczana jako:

$$P_d[l] = \frac{1}{2}\left(I^2[l] + I^2[l-1]\right). \tag{3.17}$$

Z kolei moc szumu jako:

$$P_n[l] = \left(|I[l]| - |I[l-1]|\right)^2. \tag{3.18}$$

Wtedy wartość $\frac{C}{N_0}$ to:

$$\frac{C}{N_0} = 10\log_{10}\left[\frac{P_d}{P_n \cdot T_{seg}}\right]. \tag{3.19}$$

Z kolei metoda momentów [24, 78], bazuje na drugim oraz czwartym momencie sygnału zespolonego $Z_c = I + jQ$.

$$M_2 = \overline{|Z_c|^2} \tag{3.20}$$

$$M_4 = \overline{|Z_c|^4} \tag{3.21}$$

W takim przypadku moc sygnału można obliczyć ze wzoru

$$P_d = \sqrt{2M_2^2 - M_4}, \tag{3.22}$$

a moc szumu

$$P_n = M_2 - P_d \tag{3.23}$$

Wartość $\frac{C}{N_0}$ jest również wyznaczana w oparciu o wzór (3.19).

Należy podkreślić, że wybór metody obliczania $\frac{C}{N_0}$ powinien być podyktowany tym, która z nich najlepiej estymuje prawdziwą wartość stosunku mocy fali nośnej do widmowej gęstości mocy szumu. W ramach niniejszej pracy dokonano porównania wyżej wymienionych metod, które stanowi fragment następnego rozdziału rozprawy.

3.3 Weryfikacja koncepcji systemu antyspoofingowego

Intencją niniejszego rozdziału było przedstawienie założeń koncepcyjnych proponowanego systemu antyspoofingowego GPS. Określenie słuszności tej koncepcji i ocena efektywności przyjętych rozwiązań, wymagają przeprowadzenia badań naukowych, którym poświęcono dalszą część rozprawy doktorskiej. W pierwszej kolejności opisano metodykę i wyniki wykonanych badań symulacyjnych. Następnie przedstawiono sposób realizacji stanowiska pomiarowego, obejmującego praktyczną implementację systemu antyspoofingowego. W ostatniej części omówiono założenia

i przeanalizowano uzyskane wyniki badań pomiarowych, stanowiących empiryczną weryfikację koncepcji i rezultatów symulacji.

Rozdział 4

Badania symulacyjne systemu antyspoofingowego

Jak już wspomniano, pierwszy etap weryfikacji koncepcji proponowanego rozwiązania antyspoofingowego ma charakter badań symulacyjnych. Niniejszy rozdział został poświęcony ich opisowi. Głównym celem tych badań jest wstępne oszacowanie wartości parametrów, które decydują o efektywności tego systemu.

W pierwszej części rozdziału scharakteryzowano model symulacyjny, który określa teoretyczne warunki pracy systemu antyspoofingowego. Założenia przyjęte w tym modelu mają wpływ na wartości uzyskiwanych wyników symulacji.

Następnie, uzasadniono wybór środowiska do symulacji komputerowych, a także wyszczególniono części składowe opracowanego symulatora.

W kolejnym punkcie przedstawiono wyniki wstępnych badań symulacyjnych dotyczących trzech, opisanych w poprzednim rozdziale, algorytmów obliczania $\frac{C}{N_0}$. W oparciu o wyniki dokonano wyboru jednego z tych algorytmów.

Czwartą część rozdziału poświecono symulacjom, mającym na celu określenie charakterystyk błędu estymacji opóźnień fazowych, od których dokładności zależy poprawność działania

procedur antyspoofingowych.

Znajomość rozkładu ww. błędu była wymagana do przeprowadzenia właściwych badań efektywności wykrywania i eliminacji spoofingu, które zostały opisane w dwóch ostatnich punktach niniejszego rozdziału.

4.1 Model symulacyjny

Można wyróżnić dwa zasadnicze elementy modelu symulacyjnego, który został użyty w zrealizowanych badaniach. Pierwszym z nich jest model kanału radiowego, który określa charakter oddziaływania tego kanału na sygnały przesyłane od satelitów do odbiornika GPS. Drugim elementem jest model szyku antenowego, precyzujący liczbę elementów antenowych oraz ich konfigurację przestrzenną.

4.1.1 Model kanału radiowego

Postać, nadawanych w pasmie L1, cywilnych sygnałów GPS można opisać wzorem (4.1), jako iloczyn bipolarnej sekwencji impulsów danych nawigacyjnych $D(t)$, bipolarnej sekwencji impulsów ciągu pseudolosowego C/A $C_{C/A}(t)$ oraz fali nośnej o częstotliwości f_n równej 1575,42 MHz[1].

$$s_{nad}(t) = \sqrt{2P_{nad}} \cdot D(t) \cdot C_{C/A}(t) \cdot cos(2\pi f_n t), \tag{4.1}$$

gdzie P_{nad} jest mocą sygnału na wyjściu nadajnika. Sygnał docierający do odbiornika GPS jest poddany działaniu szumów i innych zakłóceń występujących w kanale radiowym, jak również szumów własnych odbiornika. Widmo zakłóceń wąskopasmowych jest rozpraszane w odbiorniku, zatem ich wpływ można uwzględnić w modelu w sposób równoważny, jako oddziaływanie szumu białego o takiej samej mocy. Wyjątek stanowią zakłócenia, których składowe częstotliwościowe występują na częstotliwości nośnej sygnału odbieranego oraz na częstotliwościach oddalonych od niej o wielokrotności 1 kHz [6]. Stosunek mocy sygnału do zakłóceń po skupieniu widma

[1] W rzeczywistości częstotliwość nośna jest nieco mniejsza, z uwagi na konieczność uwzględnienia efektów relatywistycznych

jest określany przy użyciu parametru $\frac{C}{N_0}$ (vide wzór (1.2)). W modelu przyjęto, że składowa reprezentująca szumy i zakłócenia, wpływająca na jakość prawdziwych, jak i fałszywych sygnałów GPS, będzie reprezentowana jako addytywny biały szum gaussowski (AWGN). Moc tego szumu jest dobrana w taki sposób, aby $\frac{C}{N_0}$, wyznaczone po korelacji w odbiorniku, odpowiadało zakresowi wartości obserwowanemu w warunkach rzeczywistych. Częstotliwość nośna sygnału odbieranego jest inna niż nadawanego, z uwagi na efekt Dopplera, wywołany nieustannym przemieszczaniem się satelity względem odbiornika. Należy także uwzględnić opóźnienie transmisji τ_{prop}, proporcjonalne do długości trasy propagacji, które jest uzależnione od tego, przez który element antenowy szyku jest odbierany sygnał. Zatem, postać sygnału na wejściu m-tej anteny odbiorczej opisuje poniższy wzór:

$$s_{odb,m}(t) = \sqrt{2P_{odb,m}} \cdot D(t-\tau_{prop,m}) \cdot C_{C/A}(t-\tau_{prop,m}) \cdot cos(2\pi(f_n+f_D)(t-\tau_{prop,m})) + \eta(t), \quad (4.2)$$

gdzie $P_{odb,m}$ jest mocą sygnału odbieranego, f_D jest odchyłką Dopplera częstotliwości nośnej, a $\eta(t)$ reprezentuje szumy i inne zakłócenia.

Z punktu widzenia wykrywania i eliminacji spoofingu istotne są względne opóźnienia pomiędzy sygnałami odbieranymi przez różne elementy szyku antenowego. W odniesieniu do czasu transmisji elementów sekwencji danych (20 ms) i ciągu C/A (ok. 1 μs), opóźnienia te są pomijalnie małe (poniżej 1 ns). Z kolei w odniesieniu do fali nośnej mogą być zapisane jako jej opóźnienia fazowe. Ostatecznie, przebieg sygnału dobieranego można, bez utraty ogólności, zapisać jako:

$$s_{odb,m}(t) = \sqrt{2P_{odb,m}} \cdot D(t) \cdot C_{C/A}(t) \cdot cos(2\pi(f_n + f_D)t + \phi_1 + \Delta\phi_{1,m}) + \eta(t), \quad (4.3)$$

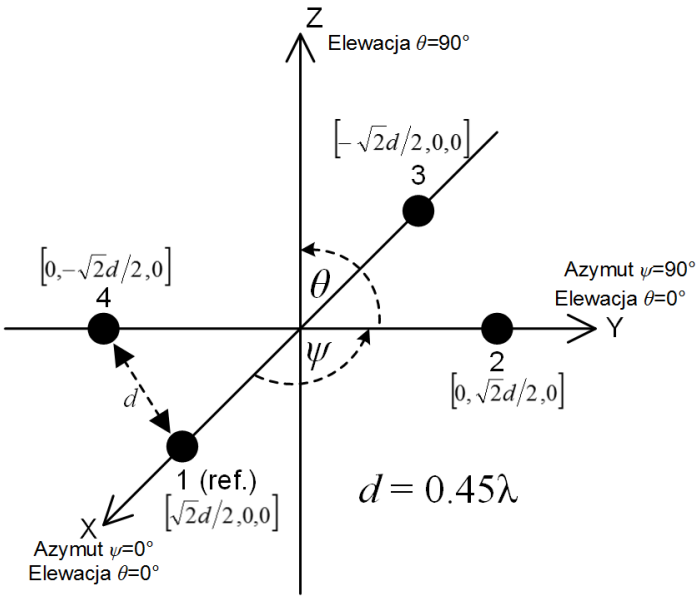
gdzie ϕ_1 jest fazą początkową fali nośnej na wejściu pierwszego elementu antenowego, a $\Delta\phi_{1,m}$ jest opóźnieniem fazowym pomiędzy elementem pierwszym i m-tym.

4.1.2 Model szyku antenowego

W badaniach przyjęto konfigurację szyku antenowego złożoną z czterech elementów. Wprawdzie opóźnienia fazowe mogą być wyznaczone nawet z użyciem dwóch anten [52], jednak, aby ograniczyć niejednoznaczność fazy, zdecydowano się rozszerzyć układ o dwa dodatkowe elemen-

ty. Znane są przykłady realizacji czteroelementowych szyków antenowych, służących do przeciwdziałania zagłuszaniu w systemach GNSS [11, 17].

Im większa liczba elementów, tym większa efektywność detekcji spoofingu i filtracji przestrzennej. Z drugiej strony, więcej sygnałów wymaga większej mocy obliczeniowej do ich przetwarzania [41]. Ponadto, przy ograniczonych wymiarach fizycznych szyku, umieszczenie elementów blisko siebie powoduje wzrost sprzężeń pomiędzy nimi, co może mieć wpływ na jakość odbieranych sygnałów.



Rysunek 4.1: Konfiguracja elementów w szyku antenowym

Oprócz liczby elementów antenowych, duże znaczenie ma ich ułożenie. Często stosowane są szyki jednorodne, w których odległości pomiędzy sąsiednimi elementami są takie same. Popularne są układy liniowe i planarne, jak również kołowe [15]. W przypadku estymacji kierunku nadejścia sygnału w dwóch płaszczyznach, korzystne może być zastosowanie układów o konfiguracji trójwymiarowej [12]. Rozmieszczenie elementów antenowych, przyjęte w niniejszej pracy, zostało przedstawione na Rys. 4.1. Elementy są ulokowane w wierzchołkach kwadratu o boku równym 0,45 długości fali nośnej o częstotliwości 1575,42 MHz. Odpowiada to odległości

równej ok. 86 mm. Odległości większe niż połowa długości fali skutkowałyby niejednoznacznością pomiaru opóźnień fazowych, co oznacza, że takie same opóźnienia fazowe mogłyby wystąpić dla sygnałów o różnych kierunkach nadejścia. Dodatkowo, przyjęto tutaj margines 0,05 długości fali, aby ograniczyć możliwość zaistnienia niejednoznaczności fazy na skutek błędu estymacji, spowodowanego m.in. obecnością szumu w kanale. Umieszczenie wszystkich elementów antenowych w jednej płaszczyźnie skutkuje tym, że wartości opóźnień fazowych sygnałów docierających z kierunków symetrycznych względem tej płaszczyzny są takie same. W praktyce nie stanowi to problemu, gdyż elementy są przytwierdzone do powierzchni przewodzącej, która odbija sygnały docierające z półprzestrzeni po tej stronie płaszczyzny, po której nie ma elementów. Płaszczyzna szyku powinna być ustawiona równolegle do powierzchni Ziemi, z elementami umieszczonymi od góry, tak aby umożliwić odbiór sygnałów GPS ze wszystkich kierunków, dla których jest zachowana bezpośrednia widoczność satelita-odbiornik.

Układ współrzędnych, w którym mogą być wyznaczane kierunki nadejścia sygnału, został określony w następujący sposób. Oś X przechodzi przez środki elementów antenowych 1 i 3 i jest skierowana w stronę elementu 1. Osie Y i Z są zorientowane z zachowaniem prawoskrętności układu współrzędnych. Kierunek nadejścia sygnału jest określony przez parę kątów azymutu i elewacji (ψ, θ). Zerowy kąt azymutu jest wyznaczony przez oś X i narasta w kierunku osi Y. Z kolei kąt elewacji jest równy 90° w kierunku osi Z, a wartość zerową osiąga w płaszczyźnie XY. W takim układzie współrzędnych, dla opisanej konfiguracji szyku antenowego, opóźnienia fazowe $\Delta\phi_{1,m}$ fali nośnej sygnału docierającego z kierunku określonego kątem azymutu ψ i katem elewacji θ , można wyznaczyć z użyciem następującej zależności:

$$\Delta\phi_{1,m} = \frac{2\pi d_{1,m}}{\lambda} cos\left[\psi + (3-m)\frac{\pi}{4}\right] cos(\theta). \tag{4.4}$$

W modelu symulacyjnym przyjęto, że charakterystyka odbiorcza wszystkich elementów antenowych ma charakter izotropowy, zatem charakterystyka całego szyku jest równa tzw. współczynnikowi układu (z ang. array factor). Charakterystyka szyku złożonego z rzeczywistych elementów może być wyznaczona w oparciu o zasadę przemnażania charakterystyk. W modelu nie zostały uwzględnione wzajemne sprzężenia elektromagnetyczne pomiędzy elementami szyku.

4.2 Środowisko symulacji komputerowych

Wszystkie badania symulacyjne zostały zrealizowane w środowisku Matlab firmy Mathworks, w wydaniu R2013a. Wybór tego programu został podyktowany dużą liczbą udostępnianych przez niego funkcji, które pozwalają na znaczące przyspieszenie tworzenia kodów źródłowych i szeroki wachlarz możliwości analizy numerycznej i graficznej uzyskanych wyników. Zrealizowany symulator ma charakter zbioru niezależnych plików skryptowych, które są interpretowane przez program Matlab. Dane wejściowe dla każdego skryptu są zapisane wprost w jego treści, lub wczytywane z zewnętrznych plików. Liczbowe wyniki symulacji są zapisywane do plików, celem ich późniejszej analizy.

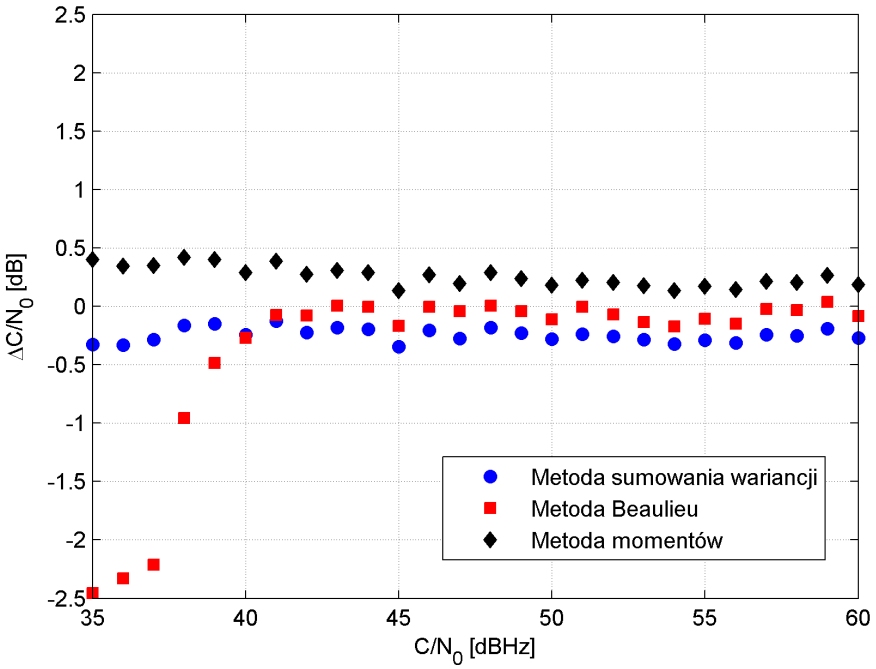
Poszczególne skrypty, składające się na symulator systemu antyspoofingowego, służą do:

- wytworzenia dyskretnych przebiegów sygnałów wejściowych symulacji,
- realizacji funkcji bloków akwizycji i śledzenia w odbiorniku GPS,
- wyznaczenia i analizy błędu estymacji opóźnień fazowych,
- analizy statystycznej kierunków nadejścia sygnałów GPS i oszacowania prawdopodobieństwa fałszywego alarmu,
- oszacowania prawdopodobieństwa detekcji spoofingu,
- analizy efektywności filtracji przestrzennej,
- analizy wpływu filtracji przestrzennej na możliwość odbioru prawdziwych sygnałów GPS.

4.3 Wybór algorytmu obliczania C/N_0

Algorytmy, które są stosowane do obliczania stosunku mocy fali nośnej do widmowej gęstości mocy szumu, umożliwiają dokonanie wymiernej oceny jakości odbieranych sygnałów. Prawidłowa estymacja jakości sygnału jest niezbędna do uzyskania charakterystyk efektywności systemu antyspoofingowego. Obliczenia $\frac{C}{N_0}$ przy użyciu różnych metod dają zbliżone, lecz nie identyczne wyniki.

W niniejszej pracy przyjęto, że estymowane wartości $\frac{C}{N_0}$ powinny możliwie najmniej odbiegać od prawdziwych w przedziale od 35 dBHz do 60 dBHz, gdyż takie wartości są obserwowane w warunkach rzeczywistych. Przeprowadzono symulacje w których obliczano $\frac{C}{N_0}$ przy użyciu: metody sumowania wariancji, metody Beaulieu i metody momentów. Uzyskane wyniki zostały przedstawione na Rys. 4.2. Jak można zauważyć, dla wartości nie mniejszych niż 40 dBHz, błąd bezwzględny w wypadku wszystkich trzech metod nie przekracza 0,5 dB. Metoda sumowania wariancji nieznacznie zaniża wynik, a metoda momentów podobnie go zawyża. Najmniejszy błąd uzyskuje się w metodzie Beaulieu, jednakże dla wartości mniejszych niż 40 dBHz przekracza on -2 dB. Biorąc pod uwagę cały rozpatrywany zakres od 35 do 60 dBHz, najmniejszy średni błąd uzyskuje się w przypadku zastosowania metody sumowania wariancji. Właśnie tę metodę wybrano do estymacji $\frac{C}{N_0}$ w niniejszej pracy.



Rysunek 4.2: Błąd $\frac{C}{N_0}$ w trzech różnych metodach estymacji

4.4 Badania charakterystyk błędu estymacji opóźnień fazowych

Przyjętym kryterium wykrycia spoofingu jest porównanie, z ustaloną wartością progową, zmierzonych różnic opóźnień fazowych fal nośnych sygnałów. Określenie parametrów jakościowych procedury detekcji wymaga zatem znajomości wielkości błędu estymacji tych różnic, którą to wielkość można wyznaczyć na podstawie charakterystyk błędu estymacji poszczególnych opóźnień fazowych.

Błąd estymacji fazy odbieranego sygnału jest zależny nie tylko od jakości odbieranego sygnału, czyli jego $\frac{C}{N_0}$, ale także od parametrów odbiornika GPS i zastosowanych w nim metod przetwarzania sygnałów. Na potrzeby realizacji badań symulacyjnych zostały napisane skrypty realizujące funkcje akwizycji i śledzenia sygnałów GPS, jak również funkcje wyznaczania opóźnień fazowych pomiędzy sygnałami z wyjść elementów szyku antenowego. Algorytmy przetwarzania sygnałów GPS w tych blokach zostały zaimplementowane zgodnie z opisem zawartym w rozdziale 3.

Aby upewnić się, że błąd pomiaru opóźnień fazowych nie zależy od kierunku nadejścia sygnału, zakres scenariuszy symulacji obejmował przypadki różnych kierunków nadejścia sygnału. Kąt azymutu był wybierany losowo jako liczba całkowita z przedziału od 0 do 359 stopni, a kąt elewacji z przedziału od 0 do 90 stopni. Dla każdego kierunku nadejścia sygnału wytworzono i zapisano, w postaci plików binarnych, próbki przebiegów czterech sygnałów, reprezentujących sygnały na wyjściach poszczególnych elementów antenowych. Sygnały drugi, trzeci i czwarty są opóźnionymi i przesuniętymi w fazie kopiami sygnału pierwszego. Wartości opóźnień sygnałów dobrano na podstawie przyjętego kierunku nadejścia, zgodnie z wzorem (4.4). Przykładowo, jeśli kąt elewacji kierunku nadejścia sygnału wynosi 90°, to wszystkie cztery sygnały są identyczne, gdyż ich względne opóźnienia są równe 0.

Wszystkie symulowane sygnały są modulowane sekwencją pseudolosową C/A przyporządkowaną pierwszemu satelicie. Parametry statystyczne ciągów przypisanych do pozostałych satelitów są takie same, więc wybór któregokolwiek z nich nie ma wpływu na ogólność uzyskiwanych wyników. Zawarta w sygnale depesza nawigacyjna ma postać naprzemiennych jedynek i zer logicznych. Taka sekwencja ułatwia weryfikację poprawności śledzenia sygnału w warun-

kach występowania przeskoków fazy w chwilach zmian bitu depeszy nawigacyjnej. Wytwarzane sygnały mają zerową odchyłkę dopplerowską, co oznacza, że zarówno fala nośna, jak i ciąg C/A oraz dane nawigacyjne, mają nominalne częstotliwości. Ciągu pseudolosowy C/A rozpoczyna się w pierwszej próbce każdego sygnału. Częstotliwość pośrednia, na której odbywa się przetwarzanie sygnałów, wynosi 2,5 MHz, a częstotliwość próbkowania jest równa 8,192 MHz. Długość każdego przebiegu wynosi 520 ms, co odpowiada 26 bitom depeszy nawigacyjnej.

Pomiar fazy sygnału GPS z pierwszego elementu antenowego jest dokonywany w trakcie fazy śledzenia tego sygnału, zgodnie z procedurą przedstawioną na Rys. 3.9. Fazy sygnałów od drugiego do czwartego są wyznaczane w podobny sposób, przy czym sygnały te nie podlegają śledzeniu, lecz są jedynie mnożone przez repliki ciągu pseudolosowego i fali nośnej, identyczne z tymi, przez które mnożony jest sygnał pierwszy. Fazy wszystkich sygnałów są wyznaczane z użyciem wzoru (3.5). Jeden zestaw wartości faz jest określany na podstawie pojedynczych segmentów sygnałów, o długości 1 ms. Zatem w jednym przebiegu procedury symulacyjnej jest wyznaczanych 520 wartości faz dla każdego z sygnałów. Na podstawie czterech wartości faz w danej milisekundzie są obliczane trzy opóźnienia fazowe, stanowiące różnice faz sygnałów z wyjść par elementów antenowych: 1 i 2, 1 i 3 oraz 1 i 4.

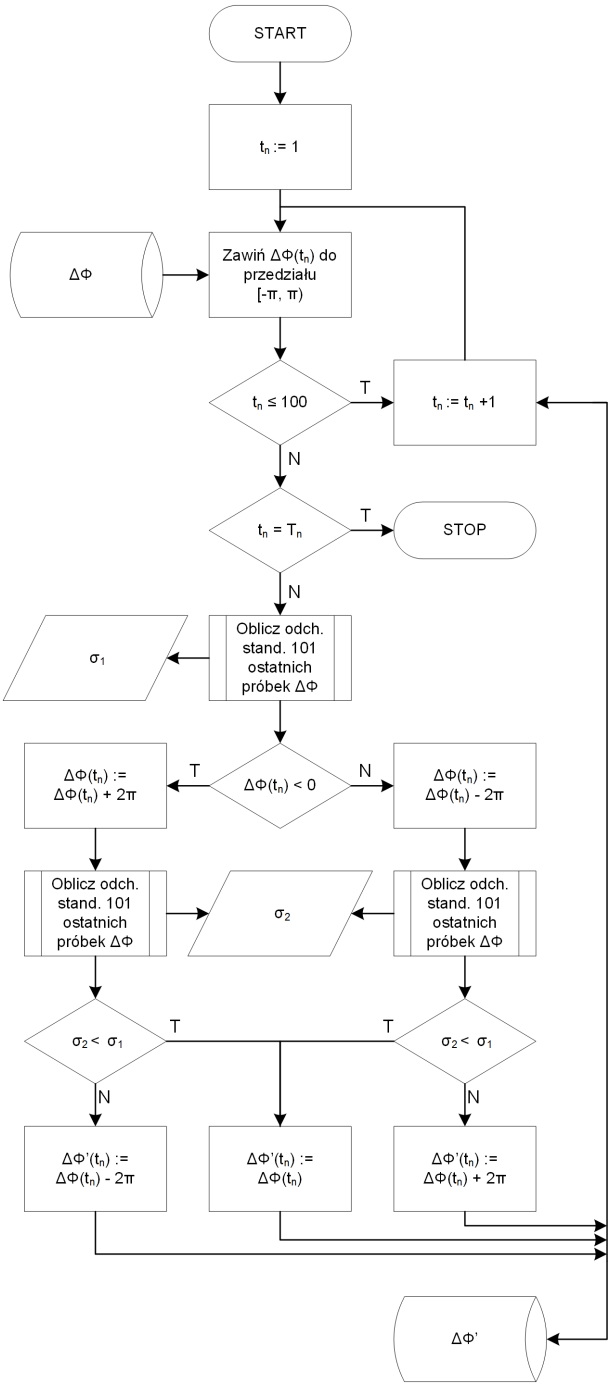
Wielkość błędu estymacji opóźnień fazowych jest określona przez dwa parametry: błąd średni $\epsilon_{\Delta\phi}$ oraz odchylenie standardowe $\sigma_{\Delta\phi}$. Błąd średni mówi o dokładności estymacji, czyli o tym, jak bardzo wartość średnia uzyskiwanych wyników odbiega od wartości prawdziwej. Jest on obliczany według wzoru:

$$\epsilon_{\Delta\phi_{1,m}} = \frac{1}{T_n} \sum_{t_n=0}^{T_n} \left(\Delta\phi_{1,m}[t_n] - \widetilde{\Delta\phi}_{1,m}[t_n] \right), \tag{4.5}$$

gdzie T_n jest całkowitą liczbą milisekund sygnału testowego (w tym wypadku 520), a $\widetilde{\Delta\phi}$ oznacza prawdziwą wartość opóźnienia fazowego w danej milisekundzie.

Odchylenie standardowe niesie natomiast informację o precyzji estymacji, czyli o rozrzucie zmierzonych opóźnień fazowych wokół wartości średniej. Jest ono obliczane w następujący sposób:

$$\sigma_{\Delta\phi_{1,m}} = \sqrt{\frac{1}{T_n} \sum_{t_n=0}^{T_n} \left(\Delta\phi_{1,m}[t_n] - \overline{\Delta\phi_{1,m}} \right)^2}. \tag{4.6}$$

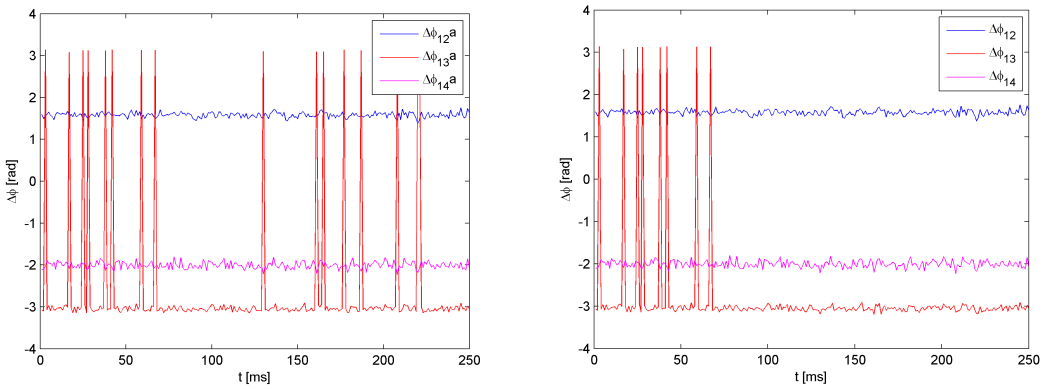


Rysunek 4.3: Schemat algorytmu wyboru przedziału odwzorowania fazy

W analizie wielkości mających charakter fazy, tak jak ma to miejsce w tym przypadku, należy zwrócić szczególną uwagę na problem przeskoków spowodowanych tzw. zawijaniem fazy (z ang. phase wrapping). Przez zawijanie fazy należy rozumieć powstawanie nieciągłości w przebiegu czasowym fazy, które są spowodowane jej odwzorowaniem do ustalonego przedziału o szerokości 2π. Przykładowo, jeśli wyznaczone opóźnienie fazowe jest odwzorowywane do przedziału $\langle -\pi, \pi)$, a prawdziwa wartość tego opóźnienia jest bliska początkowi lub końcowi tego przedziału, szum, o nawet niewielkiej mocy, może powodować częste przeskoki o $\pm 2\pi$, które znacząco zawyżają odchylenie standardowe i mogą prowadzić do wyznaczenia nieprawidłowej wartości błędu średniego. Aby ograniczyć występowanie takich przeskoków, wprowadzono adaptacyjny wybór przedziału odwzorowania fazy. Polega to na tym, że wybór przedziału, z którego wartość przyjmuje aktualne opóźnienie fazowe, jest uzależniony od poprzednich stu zmierzonych wartości tego opóźnienia i jego bieżącej wartości. W pierwszych 100 ms sygnału wszystkie opóźnienia fazowe są odwzorowywane do przedziału domyślnego $\langle -\pi, \pi)$. W przypadku kolejnych jest wykonywana procedura wyboru jednego z dwóch przedziałów. Jeśli wartość opóźnienia fazowego w przedziale domyślnym jest ujemna, jest ona dodatkowo odwzorowywana do przedziału $\langle \pi, 2\pi)$, poprzez dodanie do niej 2π. W przeciwnym wypadku, następuje dodatkowe odwzorowanie opóźnienia do przedziału $\langle -2\pi, -\pi)$, poprzez odjęcie od niego 2π. W każdym przypadku, dla każdego z dwóch wariantów, jest obliczane odchylenie standardowe wektora złożonego z aktualnej i stu poprzednich wartości opóźnienia fazowego. Ostatecznie wybierana jest ta wartość dla której odchylenie standardowe przyjmuje mniejszą wartość. Algorytm wyboru przedziału odwzorowania fazy został przedstawiony graficznie na Rys. 4.3.

Do wyznaczenia wielkości błędu estymacji uwzględniane są tylko opóźnienia fazowe począwszy od 101. ms. Również tylko te wartości są używane w procedurze wykrywania spoofingu i obliczenia współczynników wagowych filtracji przestrzennej. Na Rys. 4.4 a) i b) przedstawiono przykładowe przebiegi opóźnienia fazowego w dwóch wariantach: bez i z adaptacyjnym wyborem przedziału odwzorowania fazy. W tym przypadku nie występują przeskoki opóźnień fazy pomiędzy elementami antenowymi 1 i 2 oraz 1 i 4, w związku z czym pozostają one w przedziale $\langle -\pi, \pi)$. Z kolei opóźnienie pomiędzy elementami 1 i 3 jest bliskie $-\pi$ i wszystkie dodatnie

próbki późniejsze niż 100 ms są odwzorowywane do przedziału $\langle -2\pi, -\pi)$.

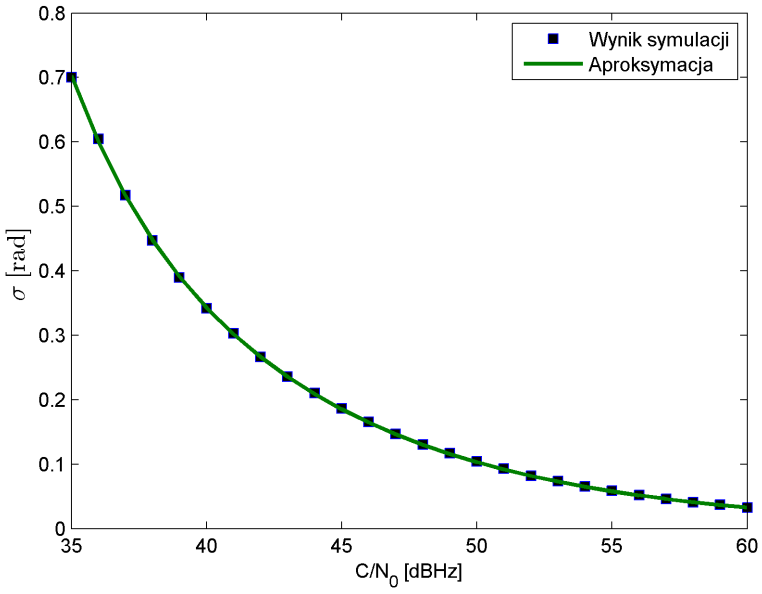


(a) (b)

Rysunek 4.4: Opóźnienia fazowe: (a) odwzorowane w ustalonym przedziale $\langle -\pi, \pi)$, (b) z adaptacyjnym wyborem przedziału odwzorowania

Charakterystyki błędu estymacji opóźnień fazowych zostały określone dla zakresu $\frac{C}{N_0}$ od 35 dBHz do 60 dBHz, co odpowiada zakresowi SNR od -28 dB do -3 dB. Rysunek 4.5 przedstawia odchylenie standardowe błędu estymacji opóźnienia fazy. Każdy punkt tej charakterystyki stanowi wartość średnią z 4200 pomiarów (10 iteracji, w każdej 420 ms). Parametry błędu estymacji opóźnień fazowych, mierzonych w trzech parach elementów antenowych, miały bardzo podobne wartości dla wszystkich badanych przypadków kierunku nadejścia sygnału. Wskazuje to na brak zależności pomiędzy prawdziwą wartością opóźnienia fazowego, a odchyleniem standardowym błędu jego estymacji. Jak wspomniano wcześniej, stanowi to przewagę estymacji fazy nad estymacją kierunku nadejścia sygnału, gdzie wielkość błędu estymacji jest zależna od tego kierunku.

Na wykresie widać wyraźny monotoniczny spadek $\sigma_{\Delta\phi}$ ze wzrostem stosunku sygnał-szum. Jak można zauważyć, dla sygnału o słabej jakości odchylenie standardowe może wynosić nawet 0,7 radiana, czyli ok. 40 stopni. Jest to spowodowane dużą wrażliwością dokładności estymacji fazy na obecność szumu. Wyznaczona charakterystyka jest zbliżona do wyników przedstawionych w [4].



Rysunek 4.5: Odchylenie standardowe błędu estymacji opóźnienia fazowego

Wyniki uzyskane dla całkowitych wartości $\frac{C}{N_0}$ stanowiły podstawę do wyznaczenia postaci funkcji opisującej tę zależność. Wzór ogólny funkcji aproksymującej ma, dobraną heurystycznie, postać:

$$\sigma_{\Delta\phi}(C/N_0) = \sqrt{10^{\left(a_1 - \frac{C/N_0}{a_2}\right)} + 10^{\left(a_3 - \frac{C/N_0}{a_4}\right)}}. \tag{4.7}$$

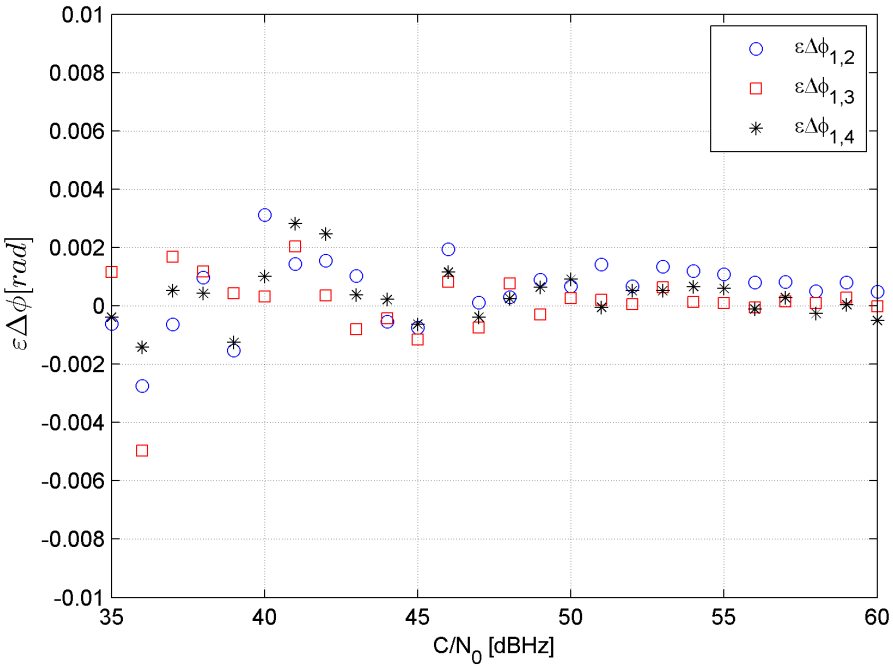
Aby znaleźć wartości parametrów od a_1 do a_4, dokonano aproksymacji metodą najmniejszych kwadratów. Do minimalizacji błędu aproksymacji posłużono się metodą optymalizacji pn. particle swarm optimization (PSO). Optymalne wartości współczynników przedstawiono w poniższej tabeli.

Tabela 4.1: Współczynniki funkcji aproksymującej $\sigma_{\Delta\phi}(C/N_0)$

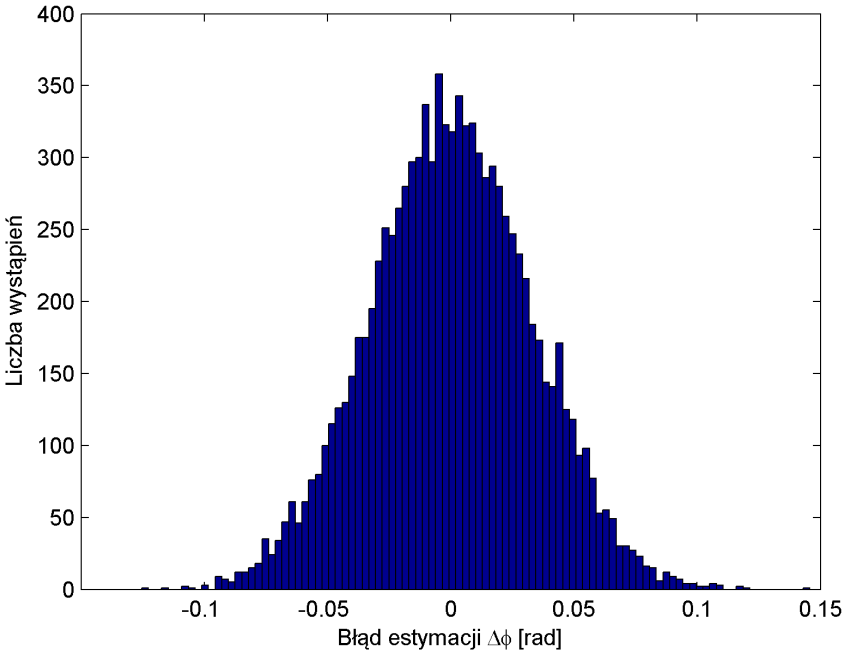
Współczynnik	Wartość	Współczynnik	Wartość
a_1	3,037	a_3	7,093
a_2	10,083	a_4	4,508

Przebieg funkcji aproksymującej został naniesiony linią ciągłą na Rys. 4.5. Wartość pierwiastka błędu średniokwadratowego aproksymacji dla całkowitych wartości $\frac{C}{N_0}$, z zakresu od 35 do 60 dBHz, wynosi $1,3 \cdot 10^{-3}$ radiana. Dowodzi to, że znaleziona postać funkcji jest dobrze dopasowana do wyników symulacji w rozpatrywanym przedziale $\frac{C}{N_0}$.

Uzyskane w symulacjach wartości błędu średniego $\epsilon_{\Delta\phi}$ estymacji opóźnień fazowych zostały przedstawione na Rys. 4.6. Podobnie jak w przypadku charakterystyk $\sigma_{\Delta\phi}$, każda z wartości stanowi średnią z 4200 wyników cząstkowych, a wyniki uzyskane dla różnych kierunków nadejścia sygnału są do siebie podobne. Wartości te są znacznie mniejsze od odchylenia standardowego. Co więcej, brak jest wyraźnej zależności pomiędzy jakością sygnału a wartością błędu. Można na tej podstawie wywnioskować, że błąd średni estymacji opóźnień fazowych jest równy zeru, a wartości niezerowe na wykresach wynikają jedynie z ograniczonej liczby uśrednień.

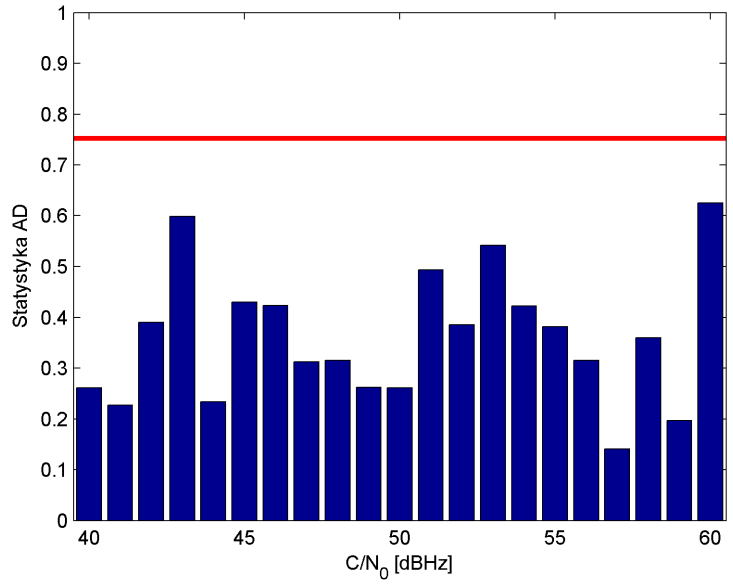


Rysunek 4.6: Błąd średni estymacji opóźnienia fazowego

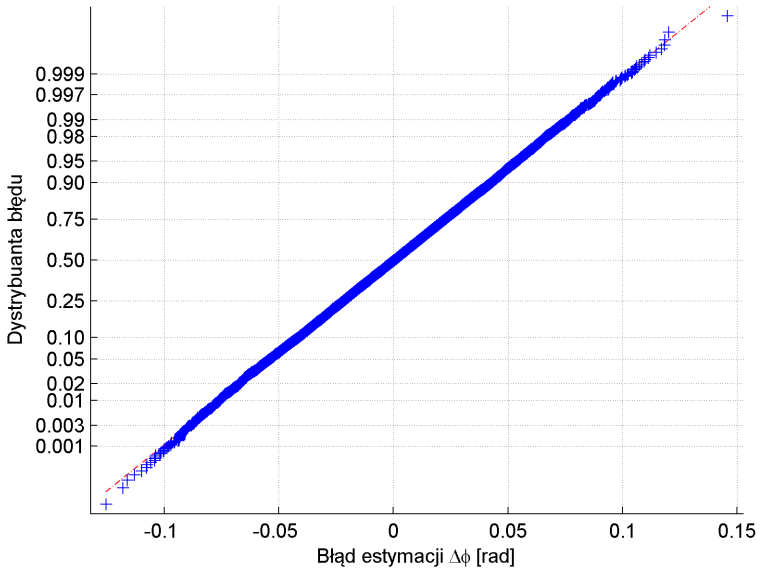


Rysunek 4.7: Histogram błędu estymacji opóźnienia fazowego (Liczba wszystkich próbek: 10000, liczba przedziałów: 100)

Pełna informacja o charakterystykach błędu estymacji opóźnienia fazowego składa się z wartości średniej i odchylenia standardowego oraz rozkładu prawdopodobieństwa tego błędu. Dyskretnym przybliżeniem ciągłego rozkładu prawdopodobieństwa błędu jest histogram wartości błędu wyznaczonych podczas symulacji. Jeden z takich histogramów, został zaprezentowany na Rys. 4.7. Wyznaczono go przy $\frac{C}{N_0} = 60$ dBHz. Ma on kształt przypominający krzywą dzwonową Gaussa. Można na tej podstawie przypuszczać, że błąd ma rozkład normalny. Aby zweryfikować tę hipotezę posłużono się testem Andersona-Darlinga [2]. Statystyka ta umożliwia określenie zgodności rozkładu uzyskanego empirycznie z pewnym rozkładem wzorcowym, w szczególności z rozkładem normalnym. Uznaje się, że rozkład empiryczny jest normalny, gdy wartość statystyki Andersona-Darlinga jest mniejsza niż ustalony próg. Na Rys. 4.8 przedstawiono wartości metryki A-D błędu estymacji opóźnień fazowych dla $\frac{C}{N_0}$ od 40 do 60 dBHz. W całym zakresie uzyskano wartości mniejsze od 0,75, stanowiącego wartość progową.



Rysunek 4.8: Wartości statystyki testu Andersona-Darlinga



Rysunek 4.9: Wykres normalny błędu estymacji opóźnienia fazowego

Oprócz statystyki Andersona-Darlinga, zgodność z rozkładem normalnym można przedstawić w sposób graficzny, przy użyciu wykresu prawdopodobieństwa normalnego, zwanego także wykresem normalnym. Na takim wykresie, skwantowane i posortowane skumulowane częstości występowania próbek są odniesione do dystrybuanty rozkładu normalnego. Skala osi rzędnych jest ustalona w taki sposób, aby wykres dystrybuanty był linią prostą. Im bardziej rozkład empiryczny jest zbliżony do rozkładu normalnego, tym bardziej uzyskane częstości pokrywają się z tą prostą. W środowisku Matlab, do narysowania wykresu normalnego można użyć wbudowanej funkcji *normplot()*. Przykładowy wykres normalny błędu estymacji opóźnień fazowych, dla $\frac{C}{N_0} = 60$ dBHz, został przedstawiony na Rys. 4.9. Jak widać, wykres jest bliski linii prostej, co pozwala stwierdzić, że rozkład błędu estymacji opóźnienia fazowego może być uznany za normalny.

4.5 Badania wykrywania spoofingu

Jak opisano w rozdziale 2.4, parametrami jakościowymi wykrywania spoofingu są prawdopodobieństwo fałszywego alarmu P_{FA} oraz prawdopodobieństwo detekcji spoofingu P_D. Opisane w tym podrozdziale badania miały na celu, po pierwsze, ustalenie progów detekcji, dla których P_{FA} jest akceptowalnie małe. Po drugie, dla ustalonych wartości progowych zostało oszacowane prawdopodobieństwo poprawnego wykrycia spoofingu.

4.5.1 Progi detekcji spoofingu

Fałszywy alarm jest sytuacją, w której spoofing jest wykryty, pomimo że w rzeczywistości atak nie jest przeprowadzany. Pozytywna decyzja o wykryciu spoofingu jest podejmowana, gdy wszystkie różnice odpowiednich opóźnień fazowych $\Phi_{i,j|s_k,s_l}$, co najmniej czterech odbieranych sygnałów GPS, są nie większe niż wartość progowa. Prawdopodobieństwo wystąpienia takiej sytuacji jest uzależnione od wielkości błędu estymacji opóźnień fazowych, który z kolei może powodować zaniżenie wartości różnic tych opóźnień. Aby oszacować to prawdopodobieństwo należy użyć wzoru (4.8). Zakłada się przy tym, że rozkłady prawdopodobieństwa różnic opóźnień

fazowych są statystycznie niezależne.

$$P_{FA} = \prod_{m=2}^{M} \prod_{k=1}^{N} \prod_{l=1, l\neq k}^{N} P\left(|\Phi_{1,m|s_k,s_l}| \leqslant \Phi_{prog}\right) \quad N \geqslant 4. \tag{4.8}$$

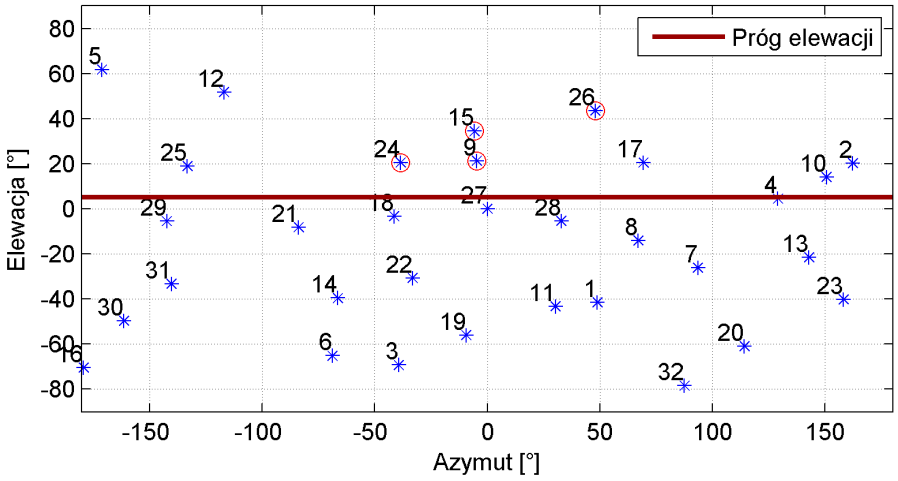
Jak można zauważyć, prawdopodobieństwo fałszywego alarmu stanowi iloczyn dystrybuant różnic opóźnień fazowych dla argumentu stanowiącego próg detekcji. Zatem do wyznaczenia tego prawdopodobieństwa, przy ustalonym kierunku nadejścia sygnału, wymagana jest znajomość charakterystyk błędu estymacji różnic opóźnień fazowych. W punkcie 4.4 przedstawiono postać błędu estymacji opóźnień fazowych. Wiedząc, że ten błąd ma rozkład normalny, można stwierdzić, że błąd estymacji różnic tych opóźnień ma również rozkład normalny. Wiadomo, że wartość średnia sumy (różnicy) niezależnych zmiennych losowych o rozkładzie normalnym jest sumą (różnicą) wartości średnich tych zmiennych. Z kolei odchylenie standardowe sumy (różnicy) takich zmiennych stanowi pierwiastek z sumy ich wariancji. Wartość średnia błędu estymacji opóźnień jest zerowa, więc wartość średnia błędu estymacji różnicy opóźnień jest również równa zeru. Jeśli chodzi o $\sigma_{\Delta\phi}$, to przyjęto tu dla uproszczenia, że wszystkie sygnały są jednakowej jakości, więc odchylenia standardowe ich opóźnień fazowych są takie same. Zatem błąd estymacji różnic opóźnień fazowych można opisać rozkładem normalnym $N\left(0, \sigma_{\Phi}^2\right) = N\left(0, \sigma_{\Delta\phi}^2 + \sigma_{\Delta\phi}^2\right) = N\left(0, 2\sigma_{\Delta\phi}^2\right)$. Korzystając ze wzoru na postać dystrybuanty rozkładu normalnego można równanie (4.8) zapisać jako:

$$P_{FA} = \prod_{m=2}^{M} \prod_{k=1}^{N} \prod_{l=1, l\neq k}^{N} \frac{1}{2}\left[1 + erf\left(\frac{\Phi_{prog} - |\overline{\Phi}_{1,m|s_k,s_l}|}{2\sigma_{\Delta\phi}}\right)\right], \tag{4.9}$$

gdzie $erf(x)$ jest funkcją błędu Gaussa. Jako że błąd średni estymacji różnic opóźnień fazowych jest równy 0, wartość średnia $\overline{\Phi}$ każdej z różnic jest równa prawdziwej wartości tej różnicy. Tę prawdziwą wartość można obliczyć w oparciu o kierunki nadejścia sygnałów, korzystając ze wzoru (4.4). Z kolei wartość $\sigma_{\Delta\phi}$ zależy od $\frac{C}{N_0}$ zgodnie z relacją (4.7).

W niniejszej pracy przyjęto, że prawdopodobieństwo fałszywego alarmu nie może być większe niż 10^{-4}, czyli że fałszywy alarm jest dopuszczalny statystycznie w jednej na 10 tysięcy prób detekcji spoofingu. Należy więc, dla każdego poziomu $\frac{C}{N_0}$ dobrać taką wartość Φ_{prog}, dla którego nie zostanie przekroczone akceptowalne prawdopodobieństwo fałszywego alarmu. Wartość te-

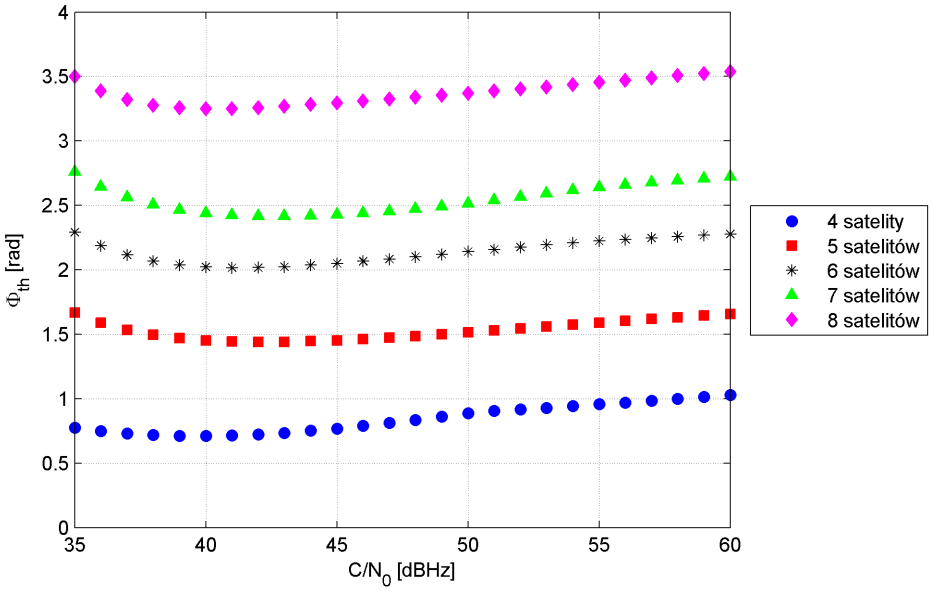
go prawdopodobieństwa jest uzależniona od wzajemnego położenia odbiornika i satelitów GPS. Fałszywy alarm jest najbardziej prawdopodobny gdy odbierane prawdziwe sygnały GPS mają podobne kierunki nadejścia. W badaniach symulacyjnych uwzględniono 1440 różnych konfiguracji pozycji satelitów GPS, obliczonych na podstawie almanachu[2], dla okresu 24 godzin z krokiem co jedną minutę. Uwzględniono także różne możliwe szerokości geograficzne, na których może znajdować się odbiornik. Przyjęto tu zakres od 0° do 90°N, z krokiem co 15°. Długość geograficzna pozycji odbiornika była równa 0°, a wysokość równa 0 m. W sumie przeanalizowano więc $7 \cdot 1440 = 10080$ różnych konfiguracji przestrzennych satelitów i odbiornika. Dla każdej z nich wyznaczano od czterech do ośmiu satelitów o najbardziej zbliżonych kierunkach nadejścia sygnału.



Rysunek 4.10: Wybór czterech satelitów o najmniejszej rozbieżności kierunków nadejścia sygnałów

[2]Almanach - zbiór podstawowych informacji o parametrach orbitalnych wszystkich satelitów w konstelacji oraz o ich statusie, odchyłkach zegara i poprawkach jonosferycznych

Na Rys. 4.10 przedstawiono przykładowy wybór czterech satelitów o najbardziej podobnych kierunkach (czerwone okręgi). Są one wybierane spośród wszystkich satelitów, dla których kąt elewacji jest większy niż tzw. maska, którą ustalono tu na 5° (linia pozioma).



Rysunek 4.11: Progi detekcji spoofingu przy odbiorze od 4 do 8 sygnałów GPS

Dla danej liczby od 4 do 8 sygnałów GPS i dla danej całkowitej wartości $\frac{C}{N_0}$ z zakresu od 35 dBHz do 60 dBHz, wybierana była minimalna wartość Φ_{prog}, spośród wartości, przy których spełniony jest warunek $P_{FA} \leqslant 10^{-4}$, obliczonych dla wszystkich analizowanych konfiguracji satelitów. Wyznaczone w ten sposób wartości progów detekcji zostały przedstawione na Rys. 4.11. Im więcej satelitów jest widocznych w punkcie odbioru, tym większa jest rozbieżność kierunków nadejścia ich sygnałów. Wyraźnie widać więc, że przy większej liczbie satelitów, wartość progu detekcji, zapewniająca takie samo prawdopodobieństwo fałszywego alarmu, jest większa, co umożliwia uzyskanie większego prawdopodobieństwa detekcji spoofingu. Analizując zależność progu od $\frac{C}{N_0}$, można stwierdzić, że minimum progu występuje pomiędzy 39 a 42 dBHz. Przy większych wartościach, ze wzrostem $\frac{C}{N_0}$ rośnie próg detekcji, przy czym wzrost ten nie przekracza 0,5 rad. W Tab. 4.2 podano dokładne wartości progów wyznaczonych dla całkowitych wartości $\frac{C}{N_0}$.

Tabela 4.2: Progi detekcji spoofingu w funkcji liczby sygnałów i ich stosunków C/N_0

Liczba sygnałów	C/N_0													
	35	36	37	38	39	40	41	42	43	44	45	46	47	
4	0.776	0.747	0.728	0.717	0.712	0.712	0.716	0.724	0.735	0.750	0.769	0.790	0.812	
5	1.666	1.590	1.534	1.495	1.469	1.452	1.444	1.440	1.441	1.446	1.453	1.462	1.473	
6	2.291	2.188	2.117	2.069	2.039	2.022	2.016	2.017	2.024	2.036	2.050	2.066	2.084	
7	2.762	2.645	2.563	2.506	2.468	2.442	2.427	2.420	2.418	2.421	2.429	2.441	2.456	
8	3.500	3.390	3.320	3.279	3.257	3.250	3.251	3.259	3.270	3.284	3.298	3.312	3.327	

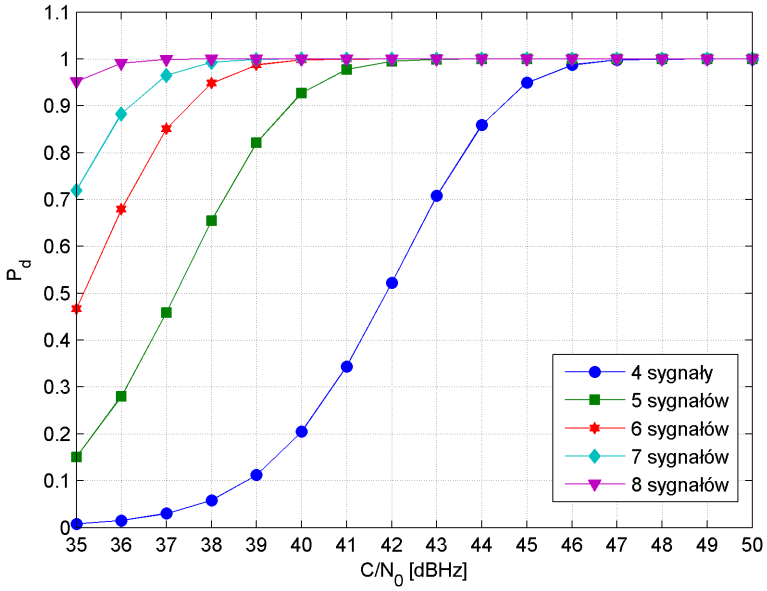
Liczba sygnałów	C/N_0													
	48	49	50	51	52	53	54	55	56	57	58	59	60	
4	0.836	0.860	0.885	0.904	0.916	0.929	0.942	0.956	0.970	0.984	0.999	1.015	1.029	
5	1.486	1.499	1.514	1.529	1.544	1.559	1.574	1.589	1.603	1.618	1.631	1.645	1.658	
6	2.102	2.121	2.140	2.159	2.176	2.193	2.208	2.222	2.235	2.247	2.258	2.267	2.277	
7	2.473	2.494	2.517	2.543	2.569	2.596	2.620	2.642	2.662	2.679	2.695	2.711	2.726	
8	3.342	3.357	3.372	3.388	3.404	3.421	3.438	3.455	3.473	3.490	3.507	3.523	3.538	

4.5.2 Prawdopodobieństwo detekcji spoofingu

Przy ustalonych wartościach progu detekcji jest możliwe oszacowanie prawdopodobieństwa P_D poprawnego wykrycia spoofingu. Stosuje się w tym przypadku wzór analogiczny do wzoru (4.9), przy czym wartości średnie różnic opóźnień fazowych są tu równe 0, gdyż wszystkie fałszywe sygnały docierają do odbiornika z tego samego kierunku. P_D jest więc wyznaczane jako:

$$P_D = \prod_{m=2}^{M} \prod_{k=1}^{N} \prod_{l=1, l\neq k}^{N} \frac{1}{2} \left[1 + erf\left(\frac{\Phi_{prog}}{2\sigma_{\Delta\phi}} \right) \right]. \tag{4.10}$$

Obliczone, w oparciu o powyższy wzór, prawdopodobieństwa detekcji w funkcji $\frac{C}{N_0}$ zostały przedstawione graficznie na Rys. 4.12. Uwzględniono tu jedynie zakres $\frac{C}{N_0}$ od 35 dBHz do 50 dBHz, gdyż, dla większych wartości, P_D, niezależnie od liczby odbieranych fałszywych sygnałów, jest równe 1.



Rysunek 4.12: Prawdopodobieństwo poprawnej detekcji spoofingu

W Tab. 4.3 podano minimalne wartości $\frac{C}{N_0}$ fałszywych sygnałów, przy których prawdopodobieństwo poprawnego wykrycia spoofingu jest nie mniejsze niż 99%.

Tabela 4.3: Minimalne wartości $\frac{C}{N_0}$ wymagane do uzyskania $P_D \geqslant 99\%$

Liczba fałszywych sygnałów	Minimalne $\frac{C}{N_0}$ [dBHz]
4	46
5	41
6	39
7	38
8	36

Aby spoofing był skuteczny, sygnały fałszywe muszą być silniejsze od prawdziwych. Wobec tego, należy spodziewać się ich stosunkowo dużych wartości $\frac{C}{N_0}$. Jeśli będą one przekraczać 45 dBHz (SNR = -18 dB), będzie można jednoznacznie podjąć decyzję o obecności spoofingu, nawet jeśli będą nadawane jedynie cztery fałszywe sygnały GPS.

4.6 Badania filtracji przestrzennej

Jak wiadomo, zadaniem filtracji przestrzennej w metodzie kształtowania zer jest selektywne wytłumienie sygnałów niepożądanych, docierających z określonego kierunku. Celem opisanych poniżej badań symulacyjnych było stwierdzenie, jak duży poziom tłumienia sygnałów niepożądanych można uzyskać przy zastosowaniu przyjętej konfiguracji szyku antenowego. Ponadto, został zbadany wpływ filtracji przestrzennej na stosunek sygnał-szum sygnałów użytecznych. Jest to istotne z punktu widzenia możliwości odbioru fałszywych sygnałów w obecności spoofingu.

4.6.1 Tłumienie sygnałów spoofera

Wektor wag, używany do fazowania szyku celem realizacji filtracji przestrzennej, jest wyznaczany według wzoru (2.2), na podstawie zmierzonych opóźnień fazowych. Filtracja przestrzenna jest przeprowadzana w pasmie podstawowym według wzoru (3.1). Dla sygnału odbieranego, mającego postać sinusoidy zespolonej o jednostkowej mocy i częstotliwości f, postać

sygnału na wyjściu filtru przestrzennego można opisać wzorem:

$$s_{fp}\left(\psi,\theta,\overrightarrow{\mathbf{w}},f,t\right)=\sqrt{2}e^{-i\cdot\phi_c(t)}+\sqrt{2}\sum_{m=2}^{M}w_m\cdot e^{-i\cdot\gamma_m(\psi,\theta,f,t)}, \tag{4.11}$$

gdzie ψ i θ są azymutem i elewacją kierunku nadejścia sygnału, ϕ_c jest fazą początkową fali nośnej, mierzoną w pierwszym elemencie antenowym, w_m jest m-twym współczynnikiem wagowym filtracji przestrzennej, $d_{1,m}$ jest odległością pomiędzy pierwszym a m-tym elementem antenowym i $\lambda={}^{c}/_{f}$ jest długością fali. Wartości współczynników γ_m są uzależnione od struktury przestrzennej szyku antenowego. Dla postaci szyku określonej w przyjętym modelu symulacyjnym, można je wyznaczyć korzystając z poniższego wzoru:

$$\gamma_m(\psi,\theta,f,t)=\left[\phi_c(t)+\frac{2\pi d_{1,m}}{\lambda(f)}cos\left(\psi+(3-m)\frac{\pi}{4}\right)cos(\theta)\right]\quad m=2,3,4. \tag{4.12}$$

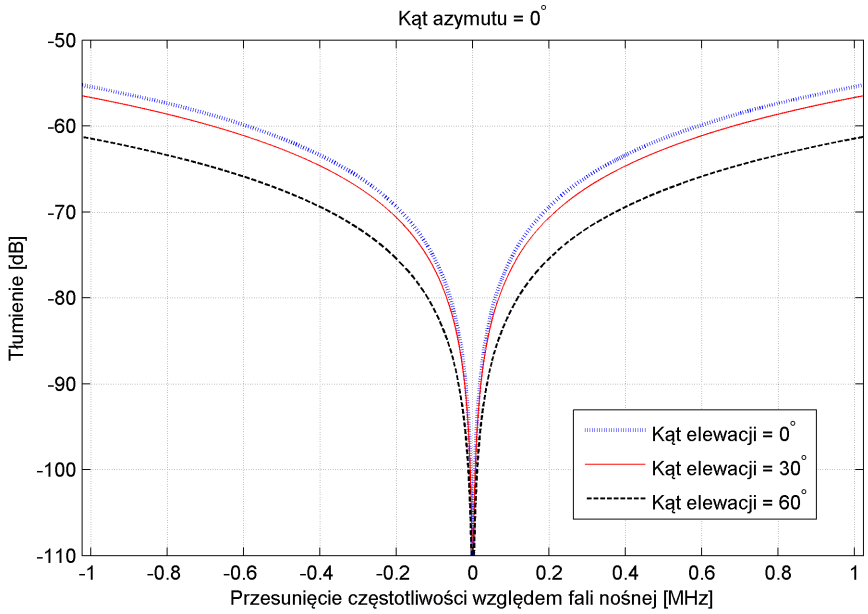
Zakładając izotropową charakterystykę wszystkich elementów antenowych, wypadkową charakterystykę kierunkową szyku można wyznaczyć jako średnią moc sygnału na wyjściu filtru przestrzennego:

$$G\left(\psi,\theta,\overrightarrow{\mathbf{w}},f\right)=\frac{1}{T}\int_{0}^{T}\left[Re\left\{s_{fp}\left(\psi,\theta,\overrightarrow{\mathbf{w}},f,t\right)\right\}\right]^2dt, \tag{4.13}$$

gdzie $T=\frac{1}{f}$.

Sygnał o widmie bezpośrednio rozproszonym, jakim jest sygnał GPS, można potraktować jako nieskończoną sumę składowych harmonicznych w pasmie o określonej szerokości. Charakter takiego sygnału jest pesudoszumowy, w związku z czym jego widmową gęstość mocy można uznać za stałą w całym pasmie. Tłumienie poszczególnych składowych częstotliwościowych w procesie filtracji przestrzennej jest różne. Jest to spowodowane tym, że wektor wag jest ustalany w oparciu o opóźnienia fazowe wyłącznie fali nośnej. Opóźnienia fazy składowych sygnału o innych częstotliwościach nie są takie same, w związku z czym ich tłumienie jest mniejsze. Różnice w tłumieniu poszczególnych składowych częstotliwościowych sygnałów są uzależnione od kierunku nadejścia tych sygnałów. Na Rys. 4.13 przedstawiono charakterystyki częstotliwościowe filtru przestrzennego dla trzech różnych kierunków nadejścia sygnału - o zerowym azymucie i kątach elewacji 0°, 30° i 60°. Jak widać, dla przyjętego modelu szyku, im mniejszy jest kąt

elewacji, tym większe są różnice w tłumieniu składowych częstotliwościowych i, co za tym idzie, mniejsze całkowite tłumienie sygnału.



Rysunek 4.13: Charakterystyki częstotliwościowe filtru przestrzennego

Aby wyznaczyć charakterystykę G_{GPS} tłumienia szerokopasmowego sygnału GPS w procesie filtracji przestrzennej, należy scałkować (4.13) po częstotliwości w pasmie $B_{GPS\ C/A}$ o szerokości 2,046 MHz wokół częstotliwości nośnej.

$$G_{GPS}\left(\psi,\theta,\overrightarrow{\mathbf{w}}\right) = \int\limits_{B_{GPS\ C/A}} G\left(\psi,\theta,\overrightarrow{\mathbf{w}},f\right) df \tag{4.14}$$

Gdy sygnał dociera z kierunku prostopadłego do płaszczyzny szyku (elewacja 90°), opóźnienia fazowe są zerowe niezależnie od częstotliwości i wszystkie składowe mogą być wytłumione zupełnie, tak jak fala nośna. Z kolei najmniejsze całkowite tłumienie, wynoszące -60 dB, występuje przy elewacji 0°, dla sygnałów GPS docierających z azymutów 0° i 180°.

Powyższe rozważania dotyczą sytuacji, gdy opóźnienia fazowe sygnałów spoofera są wyznaczane bezbłędnie. W warunkach rzeczywistych szumy i interferencje powodują błędy esty-

macji, opisane w podrozdziale 4.4. Wektor wag obliczony na podstawie błędnych wartości $\Delta\phi$ nie umożliwia uzyskania optymalnego kształtu charakterystyki odbiorczej. Nie ma ona w takim przypadku wyraźnego zera na kierunku, z którego nadchodzą fałszywe sygnały. W rezultacie sygnały te są tłumione znacznie słabiej, co może być niewystarczające do umożliwienia odbioru sygnałów prawdziwych. W przypadku gdy jest wiadomo, że sygnały spoofera nadchodzą przez cały czas z tego samego kierunku, błąd estymacji opóźnień fazowych można zmniejszyć przez uśrednianie kolejnych pomiarów. Z kolei gdy kierunek nadejścia zmienia się, zero charakterystyki należy kształtować adaptacyjnie, a wtedy uśrednianie nie jest wskazane, gdyż zwiększa bezwładność takiej adaptacji. W takim wypadku, metodą poprawy tłumienia fałszywych sygnałów może być optymalizacja położenia zera charakterystyki w oparciu o zmierzone, w danej chwili, opóźnienia fazowe. Polega to na tym, że poszukuje się kierunku nadejścia sygnału, który jest najbardziej dopasowany do zmierzonych opóźnień fazowych, a następnie ustala zero charakterystyki na tym kierunku. Jako funkcję celu Γ można tu zastosować np. wartość średnią kwadratów różnic opóźnień fazowych teoretycznych i zmierzonych:

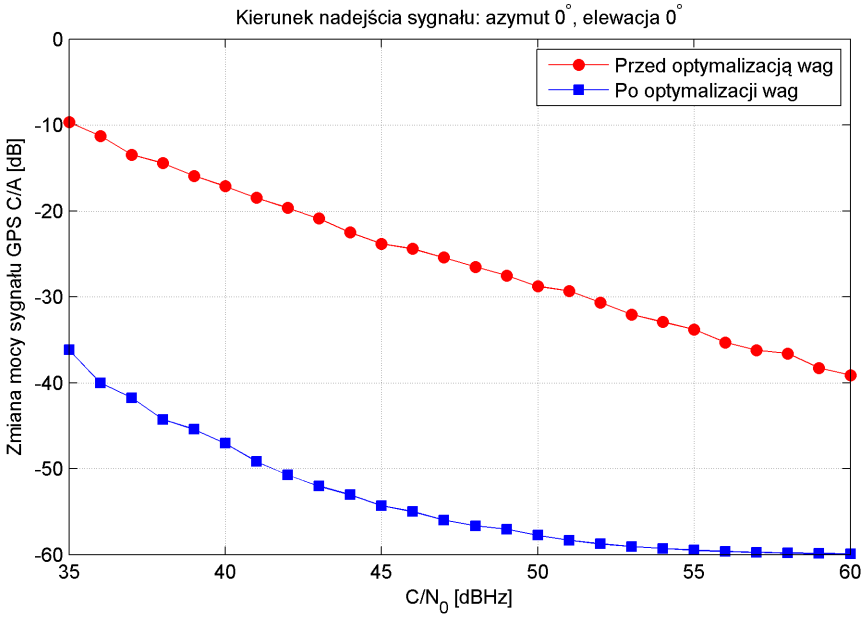
$$\Gamma(\psi,\theta) = \frac{1}{M-1}\sum_{m=2}^{M}\left[\Delta\phi_{1,m}(\psi,\theta) - \Delta\widehat{\phi}_{1,m}\right]^2, \tag{4.15}$$

gdzie $\Delta\phi(\psi,\theta)$ są opóźnieniami fazowymi wyznaczonymi, według wzoru (4.4), dla konkretnego kierunku nadejścia sygnału, natomiast $\Delta\widehat{\phi}$ to, obarczone błędem, wyniki pomiaru opóźnień fazowych. Do znalezienia optymalnych wartości ψ i θ można użyć np. metody gradientu prostego. Jest to metoda iteracyjna, dla której wynik kolejnej iteracji jest uzyskiwany według poniższego wzoru:

$$\begin{bmatrix} \psi_{k+1} \\ \theta_{k+1} \end{bmatrix} = \begin{bmatrix} \psi_k \\ \theta_k \end{bmatrix} - \beta \cdot \begin{bmatrix} \frac{\partial E}{\partial \psi}(\psi_k,\theta_k) \\ \frac{\partial E}{\partial \theta}(\psi_k,\theta_k) \end{bmatrix}, \tag{4.16}$$

gdzie k jest indeksem iteracji, a β jest współczynnikiem rzeczywistym, od wartości którego jest uzależnione uzyskanie zbieżności procedury i liczba kroków niezbędnych do osiągnięcia akceptowalnie małej wartości funkcji celu. Wartości początkowe ψ_0 i θ_0 ustala się, odpowiednio, na $0°$ i $45°$. Po zakończeniu ostatniej iteracji tworzony jest nowy wektor wag, dla którego charak-

terystyka odbiorcza szyku ma zero na znalezionym, optymalnym kierunku nadejścia sygnału spoofera.



Rysunek 4.14: Tłumienie niepożądanego sygnału GPS przez filtr przestrzenny

Na Rys. 4.14 przedstawiono porównanie uśrednionych wartości tłumienia sygnału spoofera dla przypadków bez i z optymalizacją wag, w sytuacji gdy sygnał dociera z kierunku o azymucie 0° i elewacji 0°. Każda z wyznaczonych wartości tłumienia stanowi wartość średnią z 1000 wyników obliczonych dla różnych realizacji błędu estymacji opóźnień fazowych. Rozrzut tego błędu jest uzależniony od $\frac{C}{N_0}$ zgodnie z formułą (4.7). Bez optymalizacji, sygnały spoofera o niskiej jakości są tłumione przeciętnie o kilkanaście dB. Optymalizacja wag pozwala w tej sytuacji na uzyskanie poprawy tłumienia sygnałów niepożądanych w granicach od 20 dB do 30 dB. Jak widać, przy dużym stosunku $\frac{C}{N_0}$, tłumienie całkowite sięga -60 dB, co, jak wspomniano wcześniej, jest maksymalną wartością tłumienia możliwą do uzyskania w tej konfiguracji szyku dla przyjętego kierunku nadejścia sygnału.

4.6.2 Wpływ filtracji przestrzennej na odbiór prawdziwych sygnałów GPS

Negatywnym skutkiem kształtowania zer charakterystyki szyku antenowego jest możliwa degradacja jakości sygnałów użytecznych. Degradacja ta jest tym większa, im kierunek nadejścia sygnału z satelity jest bliższy kierunkowi, na którym ustalono zero. Tłumienie sygnałów prawdziwych jest obliczane analogiczne jak fałszywych, według wzoru (4.14). O możliwości odbioru sygnałów z satelitów GPS decyduje ich wartość stosunku sygnał-szum na wyjściu filtru przestrzennego. Oprócz tłumienia sygnałów użytecznych należy więc także uwzględnić zmianę mocy szumu wywołaną przez filtrację. W przypadku, gdy szumy docierające do różnych elementów antenowych są wzajemnie nieskorelowane, zmianę mocy szumu G_{szum} można wyznaczyć w prosty sposób, jako kwadrat normy wektora wagowego, czyli sumę kwadratów modułów jego elementów.

$$G_{szum}(\overrightarrow{\mathbf{w}}) = \|\overrightarrow{\mathbf{w}}\|^2 = \sum_{m=1}^{M} |\mathbf{w}_m|^2. \tag{4.17}$$

W czteroelementowym szyku antenowym, przy równej mocy sygnałów na wyjściach wszystkich elementów, moduły wag dla ustalonego jednego zera charakterystyki (Rys. 2.4), są równe $\left[1, \frac{1}{3}, \frac{1}{3}, \frac{1}{3}\right]$. Odpowiada to wzrostowi mocy szumu równemu 1.25 dB. Oznacza to, że moc szumu na wyjściu filtru filtru przestrzennego jest o jedną trzecią większa niż na wyjściu każdego z poszczególnych elementów antenowych szyku.

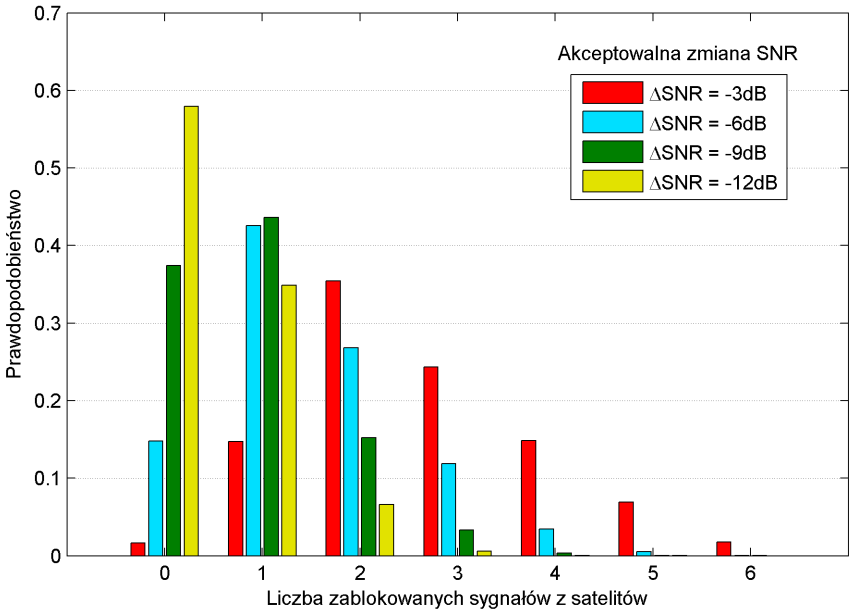
Aby obliczyć zmianę ΔSNR_{filt} stosunku mocy sygnał-szum podczas filtracji przestrzennej, należy wyznaczyć iloraz wartości G_{GPS} i G_{szum}.

$$\Delta SNR_{filt}[dB] = 10 \log \left(\frac{G_{GPS}\left(\psi, \theta, \overrightarrow{\mathbf{w}}\right)}{G_{szum}(\overrightarrow{\mathbf{w}})} \right). \tag{4.18}$$

O tym, czy prawdziwy sygnał GPS po filtracji przestrzennej może być odebrany decyduje czułość odbiornika i stosunek SNR przed filtracją. Statystyczne określenie możliwości odbioru sygnałów z satelitów wymaga sprecyzowania dopuszczalnego spadku SNR. Dla sygnałów o słabej jakości, spadek SNR nawet o jeden decybel może uniemożliwić poprawny odbiór, podczas gdy silne sygnały będą mogły być odbierane przy spadku nawet o kilkanaście decybeli.

Aby ocenić, jaka jest przeciętna liczba prawdziwych sygnałów GPS, których odbiór jest uniemożliwiony wskutek filtracji przestrzennej, przeprowadzono badania symulacyjne. Przyjęto

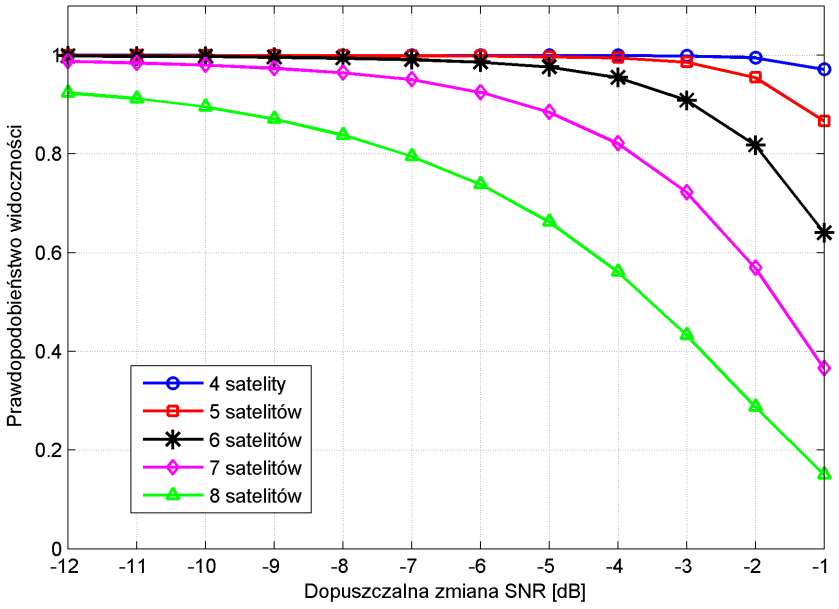
kierunki nadejścia sygnałów z satelitów takie same jak w badaniach prawdopodobieństwa fałszywego alarmu (sekcja 4.5.1). Zostało zbadanych 1297 różnych kierunków nadejścia sygnału spoofera. Kąt azymutu był wybierany z przedziału od 0° do 355° z krokiem 5°, a kąt elewacji od 0° do 85° z krokiem 5°. Uwzględniono także przypadek kąta elewacji równego 90°. Na Rys. 4.15 przedstawiono rozkład prawdopodobieństwa liczby prawdziwych sygnałów GPS wyeliminowanych przez filtrację przestrzenną. Przyjęto tu cztery wartości dopuszczalnego spadku stosunku sygnał-szum: -3 dB, -6 dB, -9 dB i -12 dB. W przypadku odbioru sygnałów o bardzo dobrej jakości, gdy akceptuje się spadek o 12 dB, w ponad połowie przypadków mogą być odbierane sygnały z wszystkich widocznych satelitów. Jednak gdy dopuszcza się spadek tylko o 3 dB, najbardziej prawdopodobna jest utrata możliwości odbioru sygnałów z dwóch satelitów.



Rysunek 4.15: Prawdopodobieństwo uniemożliwienia odbioru określonej liczby prawdziwych sygnałów GPS przez filtrację przestrzenną

Całkowita liczba satelitów widocznych na niebie jest uzależniona od pory dnia i położenia odbiornika na Ziemi. Dlatego też, z punktu widzenia użytkownika odbiornika wyposażonego

w rozwiązania antyspoofingowe, bardziej istotna niż liczba zablokowanych sygnałów z satelitów jest liczba tych sygnałów prawdziwych, które mogą być w dalszym ciągu odbierane. Aby oszacować tę liczbę, przeprowadzono kolejne symulacje, których wyniki przedstawiono na Rys. 4.16. Wykresy przedstawiają prawdopodobieństwo możliwości odbioru określonej liczby prawdziwych sygnałów GPS, w funkcji dopuszczalnego spadku wartości SNR, spowodowanego filtracją przestrzenną. Wyniki można interpretować następująco: jeśli jakość odbieranych sygnałów umożliwia ich odbiór przy spadku SNR o nie więcej niż np. 3 dB., to prawdopodobieństwo możliwości odbioru czterech, pięciu, sześciu, siedmiu i ośmiu sygnałów na wyjściu filtru przestrzennego wynosi, odpowiednio, 99,9%, 98,6%, 90,9%, 72,3% i 43,3%. Z drugiej strony, aby prawdopodobieństwo możliwości odbioru 4, 5, 6 i 7 sygnałów z satelitów GPS było nie mniejsze niż 95%, akceptowalny spadek wartości SNR nie może przekroczyć, odpowiednio, -1 dB, -2 dB, -4 dB i -7 dB. W przypadku ośmiu sygnałów, nawet dopuszczalny spadek o 12 dB zapewnia jedynie prawdopodobieństwo możliwości odbioru na poziomie 92,4%.



Rysunek 4.16: Prawdopodobieństwo możliwości odbioru określonej liczby prawdziwych sygnałów GPS po filtracji przestrzennej

Rozdział 5

Prototyp systemu antyspoofingowego

Jak to napisano wcześniej, realizacja badań symulacyjnych miała na celu wstępną ocenę efektywności przyjętych rozwiązań antyspoofingowych w warunkach modelowych. Właściwa ewaluacja parametrów systemu wykrywania i eliminacji spoofingu GPS wymaga przeprowadzenia również badań pomiarowych, do czego niezbędne jest odpowiednie stanowisko badawcze. Głównym elementem stanowiska jest prototyp systemu antyspoofingowego.

W rozdziale przedstawiono autorską realizację takiego prototypu. Omówiono zarówno warstwę jego sprzętową, jak również opracowane oprogramowanie, realizujące m.in. algorytmy wykrywania i eliminacji spoofingu.

Ostatni punkt rozdziału poświęcono opisowi użytego źródła sygnałów GPS, które również stanowi element stanowiska pomiarowego.

5.1 Założenia do realizacji prototypu

Analogicznie do modelu przyjętego w badaniach symulacyjnych, praktyczna realizacja systemu antyspoofingowego ma umożliwiać odbiór sygnałów przez cztery anteny, tworzące szyk w konfiguracji kwadratu o długości 0,45 λ.

Zdecydowano, że warstwa sprzętowa powinna być zrealizowana przede wszystkim w oparciu o gotowe urządzenia i podzespoły. Użycie takich elementów nie tylko skraca czas integracji i testowania całej konfiguracji, lecz przede wszystkim umożliwia uzyskanie powtarzalności parametrów na poziomie, który byłby trudny do osiągnięcia w przypadku samodzielnego wykonania podzespołów.

Prototyp systemu zrealizowano w technice radia programowalnego SDR. Oznacza to, że liczba analogowych bloków odbiorczych jest ograniczona do minimum, a większość procedur przetwarzania sygnałów jest wykonywana przez oprogramowanie. Takie podejście zapewnia dużą elastyczność rozwiązania. Przykładowo, korzystając z tej samej konfiguracji sprzętowej można zrealizować system wykrywania i eliminacji spoofingu dla systemów GLONASS i Galileo - wymaga to jedynie opracowania innych modułów oprogramowania. W literaturze można znaleźć przykłady, wykonanych w technice SDR, układów przeciwdziałania zakłóceniom w systemach GNSS [10].

Cyfrowe przetwarzanie sygnałów GPS jest wykonywane wyłącznie przez komputer PC. Nakład obliczeniowy związany z tym przetwarzaniem jest na tyle duży, że nie może ono być realizowane w czasie rzeczywistym, nawet pomimo zrównoleglenia obliczeń poprzez zastosowanie wielowątkowości. Zamiast przetwarzania w czasie rzeczywistym, przyjęto tu podejście sekwencyjne, w którym przetwarzane są jedynie te segmenty sygnału odbieranego, które zostały zapisane w buforze pamięci jako ostatnie. Po przetworzeniu bieżącego segmentu, analizowany jest kolejny najnowszy segment, z pominięciem próbek sygnału odebranych w trakcie przetwarzania poprzedniego segmentu. Brak możliwości analizy sygnału w czasie rzeczywistym przez komputer PC nie stanowi przeszkody do oceny efektywności przyjętych metod. Jeśli byłoby to wymagane, przetwarzanie sygnałów może być przyspieszone np. poprzez zastosowanie macierzy programowalnych typu FPGA.

Przy użyciu opisywanego prototypu można dokonać:

- pomiaru prawdopodobieństwa wystąpienia spoofingu,
- określenia liczby i numerów ciągów C/A fałszywych sygnałów GPS,
- pomiaru opóźnień fazowych fałszywych sygnałów GPS,
- realizacji filtracji przestrzennej sygnałów,
- określenia liczby sygnałów GPS odbieranych przed i po filtracji przestrzennej,
- pomiaru $\frac{C}{N_0}$ sygnałów GPS przed i po filtracji przestrzennej.

Ponadto, zakłada się dokonywanie rejestracji przebiegów sygnałów i parametrów, obserwowanych na różnych etapach przetwarzania. Rejestracja ta ma na celu umożliwienie późniejszej analizy tych sygnałów w zewnętrznym oprogramowaniu, używanym m.in. do uzyskania graficznej reprezentacji wyników.

5.2 Platforma sprzętowa prototypu

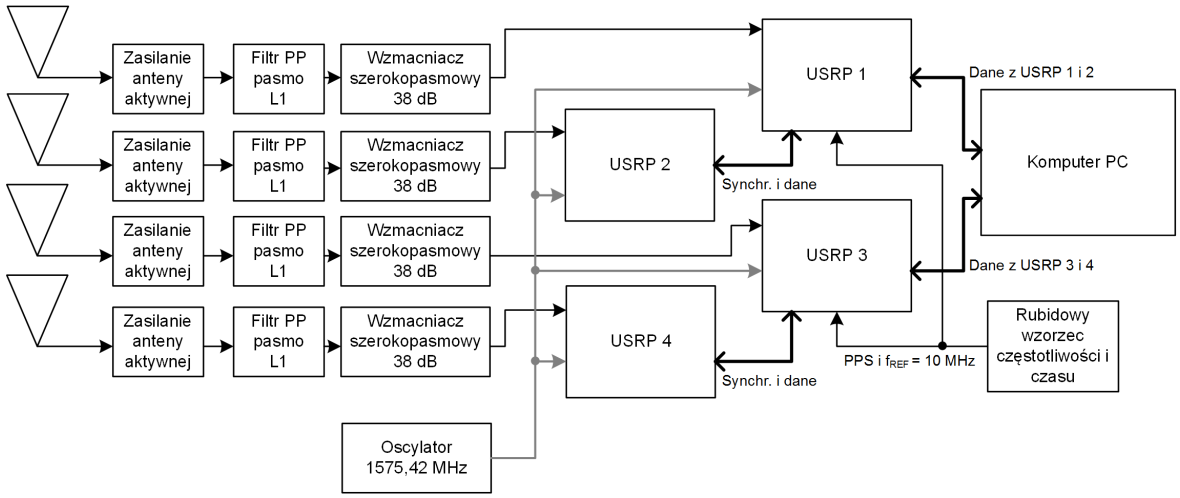
W warstwie sprzętowej prototypu można wyróżnić elementy elektroniczne analogowe, cyfrowe i mieszane. Elementy analogowe to:

- anteny aktywne tworzące płaski czteroelementowy układ antenowy oraz
- cztery tory sygnałowe w.cz. złożone z układów zasilania anten, filtrów pasmowoprzepustowych i wzmacniaczy szerokopasmowych.

Elementy analogowe służą do odbioru sygnałów w.cz. transmitowanych w pasmie L1 na częstotliwości 1575,42 MHz oraz ich wzmocnienia do poziomu odpowiadającego zakresowi napięć wejściowych przetwornika analogowo-cyfrowego.

Sygnały z wyjść wzmacniaczy są podawane na wejścia urządzeń USRP (Universal Software Radio Peripheral), które stanowią interfejs pomiędzy dziedzinami sygnałów analogowych i cyfrowych. W części analogowej te urządzenia realizują przemianę częstotliwości z pasma w.cz. (1575,42 MHz) do pasma podstawowego (0 Hz) i mogą dodatkowo wzmacniać sygnał odbierany. Następnie, sygnały są poddawane dolnoprzepustowej filtracji antyaliasingowej (niezależnie dla

składowej synfazowej I i kwadraturowej Q) i trafiają na wejścia przetworników ADC. Część cyfrowa USRP obejmuje blok kontroli transmisji próbek i pakietyzacji danych zgodnie ze standardem interfejsu Gigabit Ethernet.



Rysunek 5.1: Schemat blokowy prototypu systemu antyspoofingowego

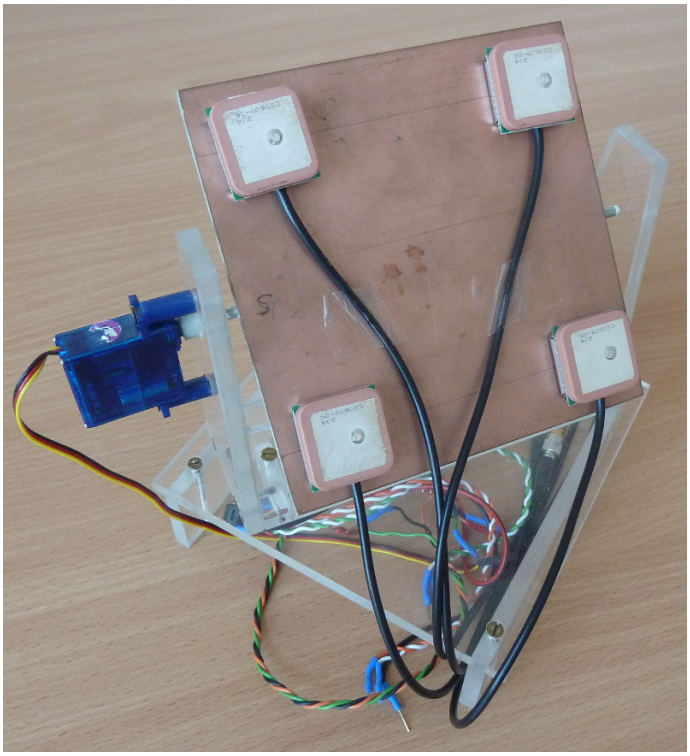
Próbki sygnałów są transmitowane do komputera PC, który realizuje zasadniczą część przetwarzania sygnałów, w tym algorytmy wykrywania i eliminacji spoofingu GPS. Schemat blokowy konfiguracji sprzętowej prototypu został przedstawiony na Rys. 5.1. Na schemacie zamieszczono również bloki oscylatora referencyjnego i rubidowego wzorca częstotliwości. Powody zastosowania tych elementów zostaną opisane w dalszej części tego rozdziału.

5.2.1 Układ antenowy

W wykonanym prototypie, sygnały GPS są odbierane przez układ antenowy złożony z czterech elementów. Zgodnie z przyjętym wcześniej modelem, anteny są rozmieszczone w taki sposób, aby ich centra fazowe stanowiły wierzchołki kwadratu o boku równym $0,45\lambda$. Długość fali nośnej o częstotliwości 1575,42 MHz wynosi ok. 19 cm, zatem minimalna odległość pomiędzy antenami w układzie wynosi ok. 8,5 cm.

W układzie zastosowano anteny firmy 2J Antennae, model 2J401GF. Są to układy aktyw-

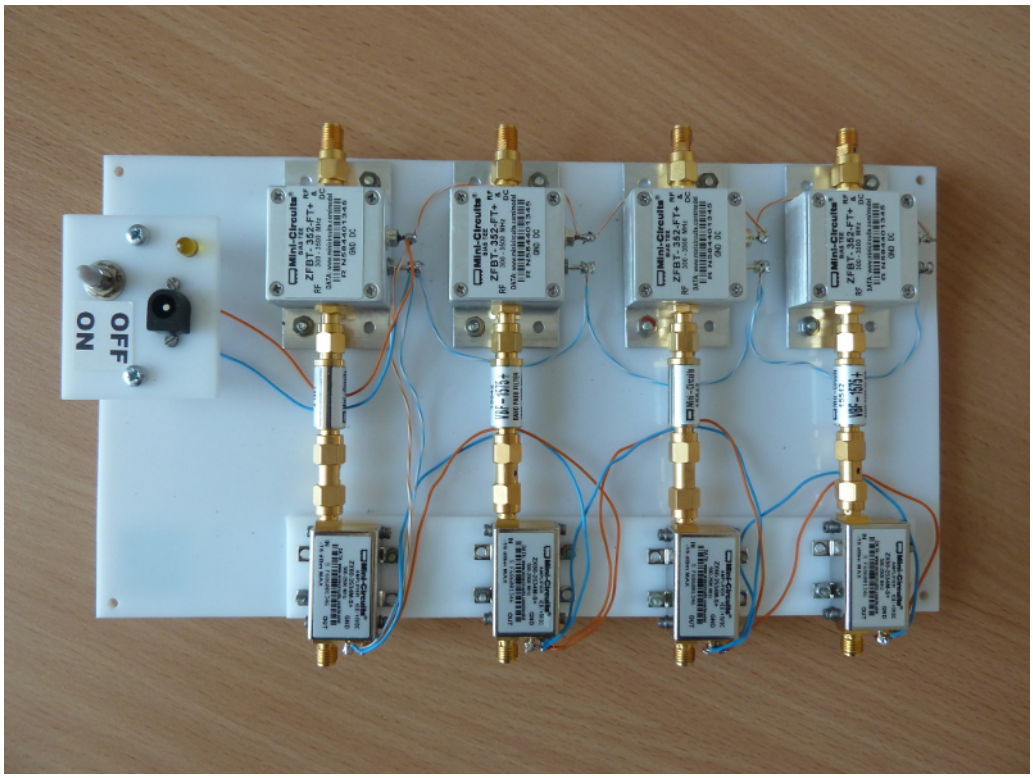
ne, które, przy zastosowanym zasilaniu napięciem 5 V, wzmacniają odbierane sygnały o 24 dB. Ponadto, mają one zintegrowany filtr pasmowo przepustowy, obejmujący pasma L1 systemów GPS i GLONASS [1]. Anteny umieszczono na płaszczyźnie przewodzącej, co eliminuje niejednoznaczność kierunku nadejścia sygnału. Układ antenowy został zamontowany na statywie, który umożliwia uzyskanie pożądanej orientacji przestrzennej przy użyciu serwomechanizmu (kąt elewacji) i silnika krokowego (kąt azymutu). Statyw ten został wykonany przez studentów Politechniki Gdańskiej, w ramach projektu grupowego [65]. Doktorant był opiekunem merytorycznym tego projektu. Widok całego układu antenowego został przedstawiony na poniższej fotografii.



Rysunek 5.2: Odbiorczy układ antenowy GNSS złożony z czterech elementów

5.2.2 Tory sygnałowe w.cz.

Wyjście każdej z czterech anten jest połączone z wejściem toru sygnałowego. Widok torów sygnałowych w. cz. został przedstawiony na Rys. 5.3. Każdy z torów jest złożony z trzech elementów, wyprodukowanych przez firmę Mini Circuits. Pierwszym elementem toru jest separator składowej stałej, który przekazuje napięcie stałe +5 V, zasilające przedwzmacniacz w antenie aktywnej, a jednocześnie przekazuje sygnał w.cz. z wyjścia tejże anteny do dalszych bloków toru sygnałowego. Zastosowano tu model ZFBT-352-FT [68].



Rysunek 5.3: Cztery analogowe tory sygnałowe w.cz.

Drugim elementem toru jest filtr pasmowo przepustowy VBF-1575, obejmujący zakres częstotliwości od 1530 MHz do 1620 MHz [67]. Jest to zakres częstotliwości obejmujący pasmo L1, w którym są nadawane sygnały systemu GPS, jak również systemów GLONASS i Galileo.

Sygnały z wyjścia filtru są wzmacniane we wzmacniaczu szerokopasmowym ZX60-2534M.

Pasmo przenoszenia tego wzmacniacza obejmuje zakres od 500 MHz do 2,5 GHz. Na częstotliwości 1,58 GHz, przy zasilaniu 5 V, jego wzmocnienie wynosi ok. 39,15 dB [69]. Po wzmocnieniu, sygnały GPS są podawane na wejście w.cz. urządzenia USRP.

5.2.3 Moduły USRP

Dla potrzeb realizacji prototypu użyto czterech urządzeń USRP firmy National Intstruments. Każde z tych urządzeń przetwarza sygnały odbierane przez inną antenę i tor w. cz. Zastosowany model NI USRP-2920 umożliwia odbiór sygnałów w zakresie częstotliwości od 50 MHz do 2,2 GHz, o szerokości pasma do 20 MHz przy próbkowaniu 16-bitowym [72]. Urządzenia te są skonfigurowane do pracy w trybie odbiorników. Każde z nich ma dwa wejścia sygnałowe, jednakże nie mogą one być używane równocześnie. Wyjścia torów w.cz. są połączone z pierwszymi wejściami sygnałowymi urządzeń USRP. Do drugich wejść sygnałowych w.cz. jest doprowadzony referencyjny sygnał harmoniczny o częstotliwości 1575,42 MHz. Sygnał ten służy do zapewnienia synchronizacji fazowej pomiędzy oscylatorami lokalnymi różnych urządzeń USRP. Z kolei synchronizacja czasowa i częstotliwościowa jest zapewniona przy użyciu atomowego rubidowego wzorca częstotliwości FS725 firmy Stanford Research Systems [91]. Wzorcowy sygnał częstotliwości 10 MHz i wzorcowy sygnał czasu PPS (jeden impuls na sekundę) są doprowadzone do odpowiednich wejść dwóch spośród czterech urządzeń USRP. Urządzenia USRP tworzą dwie pary typu master-slave. Urządzenia nadrzędne (master) są synchronizowane bezpośrednio ze wzorca rubidowego, natomiast urządzenia podrzędne (slave) są dostrajane do urządzeń master przez dedykowane kable MIMO. Kable te służą ponadto do transferu poleceń sterujących i danych użytkowych pomiędzy dwoma USRP.

Wewnętrzny mieszacz w każdym z urządzeń USRP przenosi sygnały GPS z pasma L1 do pasma podstawowego, poprzez mnożenie ich przez fale oscylatora lokalnego w kwadraturze (przesunięte względem siebie w fazie o 90°). Przetworniki analogowo-cyfrowe w USRP próbkują sygnały z częstotliwością 10 MHz. Rozdzielczość próbkowania to 16 bitów dla składowej rzeczywistej i urojonej, więc każda próbka zespolona ma rozmiar czterech bajtów. Próbki są przesyłane do komputera PC za pośrednictwem dwóch interfejsów sieciowych typu Gigabit Ethernet. Bezpo-

średnie połączenia są zestawione pomiędzy komputerem PC a dwoma USRP nadrzędnymi, które równocześnie pośredniczą w transmisji próbek z USRP podrzędnych. Widok czterech urządzeń USRP oraz rubidowego wzorca częstotliwości został zaprezentowany poniżej.

Rysunek 5.4: Cztery urządzenia USRP i rubidowy wzorzec częstotliwości

5.2.4 Komputer PC

Algorytmy odbioru sygnałów GPS, jak również algorytmy wykrywania i eliminacji spoofingu wymagają dużej liczby złożonych obliczeń. W opisywanym układzie te obliczenia są przeprowadzane przez komputer wyposażony m.in. w czterordzeniowy, 64-robitowy procesor Intel Core i7 3,2 GHz oraz w 24 GB pamięci RAM. Wielowątkowy procesor o wysokim taktowaniu umożliwia równoległe wykonywanie obliczeń w stosunkowo krótkim czasie. Z kolei duża ilość pamięci RAM pozwala tworzyć długie bufory próbek, bez konieczności ich zapisu na twardy dysk. Sumaryczna szybkość transmisji próbek z czterech urządzeń USRP do komputera wynosi 160 MB/s. Przesyłanie próbek odbywa się w sposób ciągły i jest kontrolowane przez oprogramowanie, które zostało opisane w kolejnym punkcie niniejszego rozdziału.

5.3 Oprogramowanie AntiSpoofer

Warstwę softwarową opracowanego prototypu systemu antyspoofingowego stanowi oprogramowanie o nazwie AntiSpoofer, które realizuje następujące funkcjonalności:

- odbiór i buforowanie danych z urządzeń USRP,
- akwizycja i śledzenie sygnałów GPS,
- wykrywanie spoofingu,
- filtracja przestrzenna sygnałów w przypadku wykrycia spoofingu.

Oprogramowanie zostało napisane w języku C++, a do jego kompilacji użyto programu g++ z pakietu GNU Compiler Collection. Pracuje ono pod kontrolą systemu operacyjnego Linux w dystrybucji Ubuntu 12.04.

Program AntiSpoofer jest 64-ro bitowy, co umożliwia alokację więcej niż czterech gigabajtów pamięci RAM na potrzeby przechowywania danych przez program. Ma to duże znaczenie z punktu widzenia rezerwacji pamięci dla buforów próbek odbieranych z USRP.

Interfejsem programistycznym do obsługi i komunikacji z urządzeniami USRP jest biblioteka UHD (USRP Hardware Driver) w wersji 003.006.002, opracowana przez firmę Ettus Research [23].

Oprogramowanie posiada graficzny interfejs użytkownika (GUI), wykonany przy użyciu biblioteki wxWidgets. Służy on m.in. do wyświetlania informacji o parametrach przetwarzanych sygnałów oraz informacji o wykryciu spoofingu.

5.3.1 Cykl przetwarzania sygnałów

Sygnały w postaci cyfrowej, odbierane z urządzeń USRP są przetwarzane cykliczne, gdzie w każdym cyklu jest analizowany pojedynczy segment danych. Pierwszym etapem cyklu jest skopiowanie z bufora w pamięci RAM próbek sygnału o czasie trwania 250 ms. Przy częstotliwości próbkowania 10 MHz, dla czterech urządzeń USRP daje to łącznie 10 milionów próbek. Następnie, próbki pochodzące z pierwszego USRP są zapisywane w pliku binarnym, celem ich

ewentualnej późniejszej obróbki przez oprogramowanie zewnętrzne. Próbki te reprezentują sygnał odbierany przez standardowy odbiornik GPS - bez udziału procedur antyspoofingowych.

Kolejnym krokiem jest realizacja akwizycji sygnałów GPS w oparciu o dane z pierwszego USRP. Celem akwizycji jest wykrycie sygnałów GPS odbieranych przez pojedynczą antenę. Oprócz numerów tych sygnałów, są określane ich częstotliwości Dopplera i numery próbek chwil początkowych ciągu C/A. Znajomość wartości tych parametrów jest niezbędna do przeprowadzenia kolejnego etapu przetwarzania jakim jest śledzenie sygnałów. W wyniku procesu śledzenia uzyskuje się repliki ciągów pseudolosowych i fal nośnych sygnałów GPS, odbieranych w pierwszym torze sygnałowym w.cz. Na tym etapie są także wyznaczane stosunki $\frac{C}{N_0}$ tych sygnałów.

Mnożąc sygnały z wyjść pozostałych trzech urządzeń USRP przez wspomniane repliki określa się opóźnienia fazowe pomiędzy sygnałami GPS o tych samych numerach ciągów C/A, odbieranych przez różne elementy antenowe. Dla każdego sygnału GPS są wyznaczane trzy opóźnienia, mierzone pomiędzy parami anten (parami wyjść USRP): 1 i 2, 1 i 3 oraz 1 i 4. Opóźnienia te są obliczane dla każdej milisekundy sygnału. Pierwsze 100 wartości opóźnień w każdym segmencie stanowi wektor początkowy dla procedury eliminacji zawijania fazy (Rys. 4.3) w kolejnych 150 milisekundach sygnału. Jedynie te ostanie 150 wartości, po eliminacji ewentualnych przeskoków, jest analizowane w kolejnych krokach.

Po obliczeniu opóźnień fazowych są wyznaczane ich różnice pomiędzy wszystkimi wykrytymi sygnałami GPS. Różnice opóźnień są wektorami zawierającymi 150 wartości. Liczba tych wektorów wynosi $3 \cdot N \cdot (N-1)/2$, gdzie N jest liczbą odbieranych sygnałów GPS.

Kolejnym etapem jest obliczenie prawdopodobieństwa spoofingu dla wszystkich możliwych kombinacji numerów odbieranych sygnałów, przy czym minimalna liczba numerów sygnałów w kombinacji wynosi 4. Prawdopodobieństwo spoofingu jest obliczane jako procent czasu, spośród 150 ms, w którym wszystkie różnice opóźnień fazowych są mniejsze niż ustalony próg detekcji. Wartość progu detekcji spoofingu jest określona przez minimalną wartość $\frac{C}{N_0}$ w aktualnie rozpatrywanej kombinacji sygnałów GPS. Ta kombinacja numerów sygnałów, dla której prawdopodobieństwo spoofingu jest największe, stanowi zbiór numerów fałszywych sygnałów GPS. Jeśli maksymalna wartość tego prawdopodobieństwa jest taka sama dla kombinacji o różnej

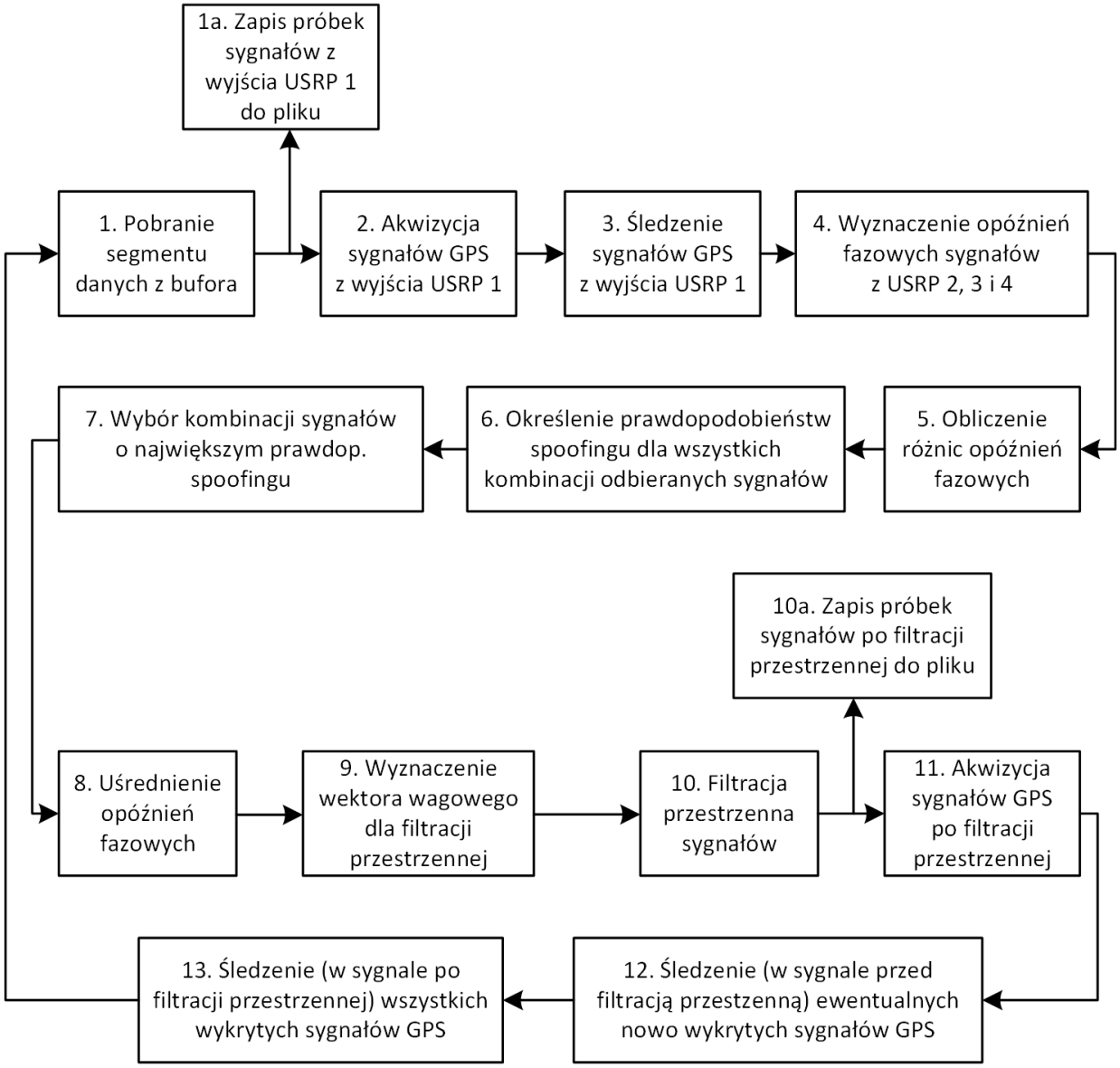
liczbie elementów, jest wybierana kombinacja o największej liczności.

Opóźnienia fazowe fałszywych sygnałów są uśredniane po czasie i numerach tych sygnałów. Ostatecznie uzyskuje się trzy średnie wartości opóźnień fazowych sygnałów spoofera pomiędzy trzema parami elementów antenowych. Te opóźnienia są podstawą do obliczenia elementów wektora wagowego, używanego w procesie filtracji przestrzennej. Filtracja przestrzenna odbywa się zgodnie z opisem w sekcji 2.3.2.

Próbki sygnału z wyjścia filtru przestrzennego są, podobnie jak próbki z wyjścia pierwszego urządzenia USRP, zapisywane w pliku, aby umożliwić ich późniejszą analizę. Jest także powtórnie wykonywana procedura akwizycji sygnałów, która ma na celu ewentualną detekcję i określenie parametrów tych prawdziwych sygnałów GPS, które nie zostały wykryte przed filtracją przestrzenną. Jeśli takie sygnały zostaną na tym etapie wykryte, jest realizowane ich śledzenie w oparciu o próbki sprzed filtracji. Przeprowadza się tę operację, aby stwierdzić jakie jakie były wartości $\frac{C}{N_0}$ tych sygnałów zanim sygnały spoofera zostały odfiltrowane. W przypadku, gdy w trakcie drugiej akwizycji zostanie wykryty sygnał GPS o takim samym numerze jak jeden z sygnałów spoofera, jest sprawdzany jego numer próbki początku ciągu C/A. Jeśli początki ciągów C/A w pierwszej i drugiej akwizycji są względem siebie przesunięte o co najmniej 5 próbek, to uznaje się, że po filtracji przestrzennej jest odbierany prawdziwy sygnał o takim samym numerze jak jeden z sygnałów spoofera.

Ostatnim etapem przetwarzania segmentu danych jest proces śledzenia wszystkich (wykrytych w trakcie obu akwizycji) sygnałów GPS po filtracji przestrzennej. W wyniku śledzenia są znane stosunki $\frac{C}{N_0}$ sygnałów na wyjściu filtru przestrzennego. Porównanie tych wartości z wartościami sprzed filtracji umożliwia ocenę efektywności eliminacji spoofingu.

Po wykonaniu powyższych operacji, z bufora pamięci jest pobierany kolejny segment próbek sygnału i rozpoczyna się kolejny cykl przetwarzania. Schemat przebiegu całego cyklu został przedstawiony na Rys. 5.5.



Rysunek 5.5: Etapy cyklu przetwarzania sygnałów w systemie antyspoofingowym

5.3.2 Kalibracja faz

Przed rozpoczęciem pierwszego cyklu przetwarzania sygnałów GPS, jest przeprowadzany proces kalibracji, którego celem jest estymacja przesunięć faz oscylatorów lokalnych USRP drugiego, trzeciego i czwartego, względem fazy oscylatora USRP pierwszego. Przesunięcia te mogą zostać następnie skompensowane, aby wyznaczone opóźnienia fazowe sygnałów odpowiadały względnym opóźnieniom sygnałów odbieranych przez różne elementy szyku antenowego.

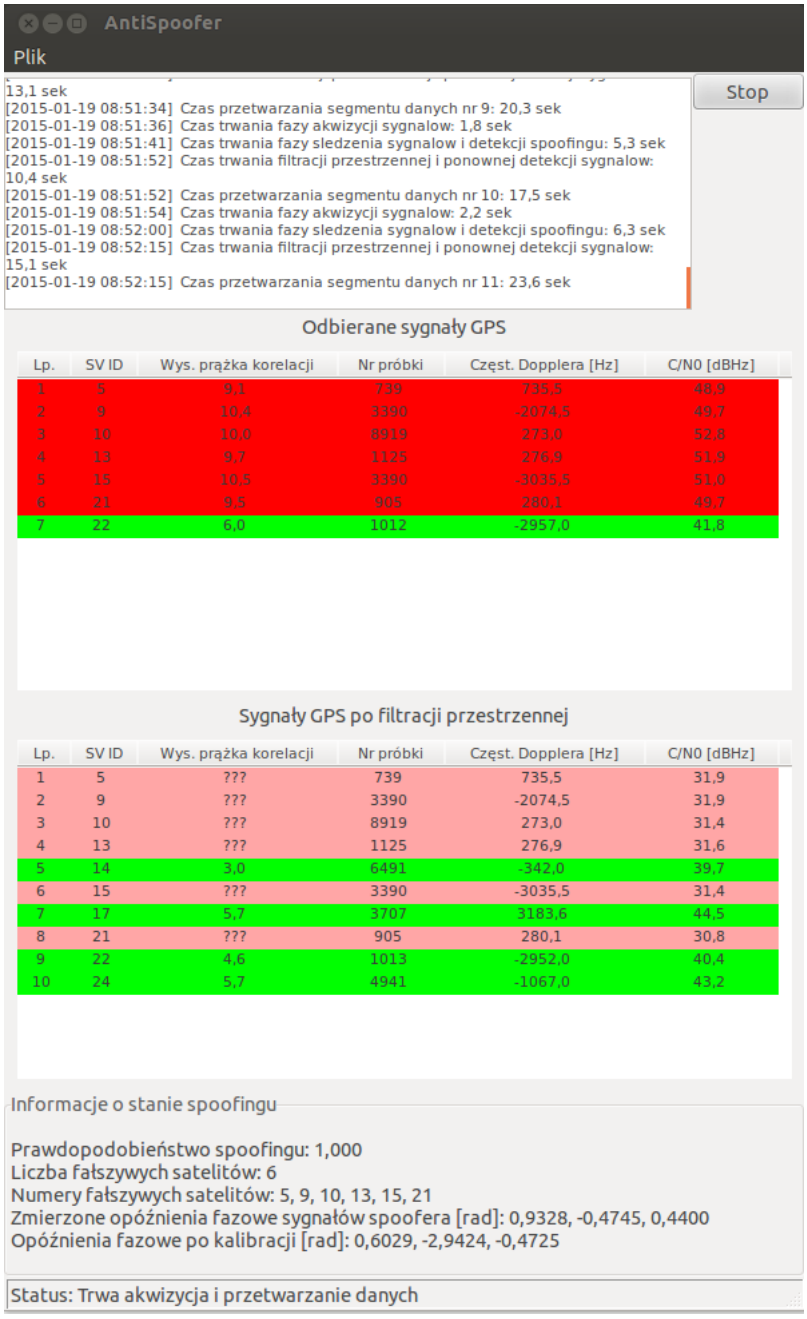
W trakcie procesu kalibracji wszystkie urządzenia USRP są ustawione na odbiór sygnałów z drugich wejść w.cz. na które jest podawany wspólny sygnał harmoniczny z oscylatora o częstotliwości 1575,42 MHz. Estymacja przesunięć fazowych jest realizowana poprzez mnożenie przez siebie próbek sygnałów zespolonych z odpowiednich wyjść urządzeń USRP.

Realizacja metod anyspoofingowych z użyciem opisywanego prototypu nie wymaga znajomości poszczególnych opóźnień fazowych sygnałów na wejściu szyku antenowego, gdyż detekcja spoofingu bazuje jedynie na różnicach tych opóźnień a filtracja przestrzenna jest realizowana w pasmie podstawowym. Co za tym idzie, kalibracja faz nie jest w tym przypadku konieczna. Jednakże przeprowadzenie takiej kalibracji byłoby wymagane np. w sytuacji gdyby były określane rzeczywiste kierunki nadejścia sygnałów GPS lub gdyby filtracja przestrzenna byłaby realizowana w sposób analogowy w pasmie w.cz., np. z użyciem regulowanych przesuwników fazy i tłumików.

5.3.3 Graficzny interfejs użytkownika

Po uruchomieniu programu AntiSpoofer, na ekranie komputera zostaje wyświetlone okno graficznego interfejsu użytkownika. Jego widok został przedstawiony na Rys. 5.6. U góry okna znajduje się pole tekstowe, w obrębie którego są wyświetlane bieżące komunikaty dotyczące działania programu. Między innymi są to informacje o konfiguracji USRP oraz o tym, ile czasu zajęło przetwarzanie poszczególnych segmentów próbek sygnału.

Na prawo od okna komunikatów umieszczono przycisk "Start/Stop". Po uruchomieniu programu jest to przycisk "Start", a jego naciśnięcie powoduje przeprowadzenie konfiguracji



Rysunek 5.6: Graficzny interfejs użytkownika programu AntiSpoofer

urządzeń USRP, a następnie uruchomienie wątku akwizycji danych z tych urządzeń oraz wątku przetwarzania tych danych w cyklu opisanym w poprzednim punkcie. Do czasu uruchomienia obu wątków przycisk jest ustawiany w tryb nieaktywny. Następnie jest on aktywowany jako przycisk "Stop". Wciśnięcie przycisku "Stop" wysyła polecenie przerwania wątków. Po zakończeniu wątków i zwolnieniu zajmowanej przez nie pamięci można zamknąć okno programu albo ponownie wcisnąć przycisk "Start".

Poniżej pola komunikatów znajdują się dwie listy z informacjami o parametrach sygnałów. Górna lista dotyczy sygnałów GPS odbieranych z użyciem pojedynczej anteny. Z kolei dolna zawiera zestawienie sygnałów GPS po filtracji przestrzennej i, w przypadku niewykrycia spoofingu, pozostaje pusta. Wpisy na obu listach składają się z tych samych elementów, tj: liczby porządkowej na liście, numeru sygnału GPS, numeru próbki rozpoczęcia ciągu C/A, częstotliwości Dopplera fali nośnej, wartości stosunku $\frac{C}{N_0}$. Na pierwszej liście, tło wpisów dotyczących odbieranych sygnałów fałszywych jest czerwone, a prawdziwych - zielone. Na drugiej liście, sygnały prawdziwe są również oznaczone kolorem zielonym, natomiast wpisy związane z wyeliminowanymi sygnałami fałszywymi mają różowe tło. Przy czym, za sygnał wyeliminowany uznaje się taki, który nie został wykryty podczas drugiej akwizycji lub którego $\frac{C}{N_0}$ po filtracji przestrzennej jest mniejsze niż 35 dBHz. Niewyeliminowane sygnały fałszywe są reprezentowane przez wpisy z czerwonym tłem. Zawartości obu list są uaktualniane bezpośrednio po zakończeniu, odpowiednio, pierwszego i drugiego procesu śledzenia sygnałów w cyklu przetwarzania (etapy 3. i 13. na Rys. 5.5).

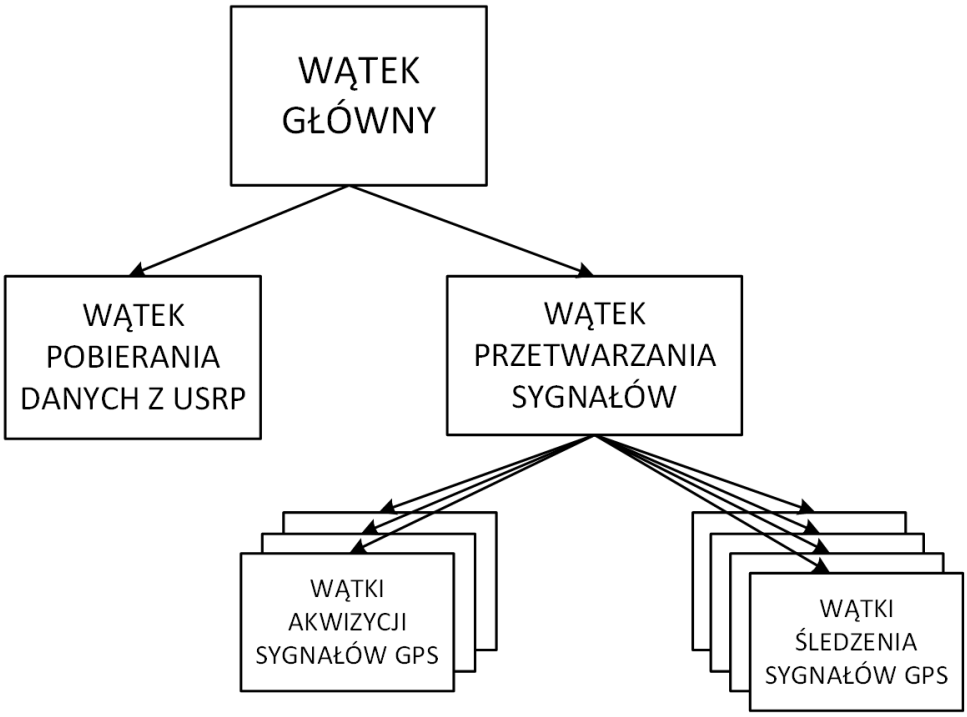
Poniżej list parametrów sygnałów GPS umieszczono panel informacji związanych z detekcją spoofingu. Są tu wyświetlane dane o: prawdopodobieństwie spoofingu, liczbie odbieranych fałszywych sygnałów, ich numerach oraz o uśrednionych wartościach ich opóźnień fazowych. Podane są dwa zestawy opóźnień fazowych - bez uwzględnienia i z uwzględnieniem kalibracji wzajemnych przesunięć fazowych oscylatorów lokalnych w urządzeniach USRP. Zawartość tego pola jest uaktualniana każdorazowo po obliczeniu opóźnień fazowych dla kombinacji numerów sygnałów GPS, dla których prawdopodobieństwo spoofingu jest maksymalne.

W dolnej części ramki okna znajduje się pasek statusu, który wyświetla aktualny stan

programu, np.: "Bezczynny", "Akwizycja i przetwarzanie danych" albo "Przerywanie wątków akwizycji i przetwarzania danych".

5.3.4 Wielowątkowość w programie AntiSpoofer

Operacje wykonywane w programie AntiSpoofer są realizowane w wielu wątkach pracy procesora komputera PC. Oznacza to, że wyodrębnione moduły programowe działają współbieżnie, a obciążenie procesora przez jeden z nich nie wpływa na szybkość działania innego.



Rysunek 5.7: Hierarchia wątków w programie AntiSpoofer

Przyjęta struktura wątków została przedstawiona na Rys. 5.7. Po uruchomieniu programu działa jedynie wątek główny, który służy głównie do obsługi interakcji użytkownika z oknem interfejsu graficznego. Wykrywa on zdarzenia wciśnięcia przycisku "Start/Stop" i wywołuje wykonanie odpowiednich akcji związanych z tymi zdarzeniami. Ponadto, w wątku głównym jest

przeprowadzana konfiguracja urządzeń USRP, po której zakończeniu są wywoływane dwa wątki podrzędne. Pierwszy z nich nieustannie odbiera próbki sygnału z czterech urządzeń USRP i zapisuje je w buforze pamięci RAM. Bufor umożliwia zapisanie 10 sekund przebiegu sygnału, po czym najstarsze próbki są nadpisywane najnowszymi. Drugi wątek podrzędny odczytuje najnowsze segmenty próbek z bufora RAM i realizuje ich przetwarzanie zgodnie z procedurą opisaną w punkcie 5.3.1. Każdorazowo, po wykonaniu określonych etapów cyklu, wątek przetwarzający dane powiadamia o tym fakcie wątek główny, który na tej podstawie aktualizuje informacje wyświetlane w GUI.

Powyższy podział na trzy wątki jest podyktowany koniecznością zapewnienia równoległej pracy różnych modułów funkcjonalnych programu (akwizycji danych, przetwarzania danych i interakcji z użytkownikiem). Wprowadzenie wielowątkowości umożliwia również znaczne skrócenie czasu wykonywania sekwencji identycznych procedur przetwarzania dla różnych danych wejściowych. Takie rozwiązanie zastosowano w tym przypadku do realizacji funkcji akwizycji i śledzenia sygnałów GPS, zarówno przed, jak i po filtracji przestrzennej. W trakcie testowania programu AntiSpoofer stwierdzono, że to właśnie wykonanie tych dwóch procedur jest najbardziej czasochłonne w całym cyklu przetwarzania. Wykonanie akwizycji zostało podzielone na trzy wątki. Pierwszy wątek poszukuje sygnałów GPS o numerach od 1 do 11, drugi od 12 do 22, a trzeci od 23 do 32. Pierwotnie miały to być cztery wątki po osiem sygnałów, jednak taki podział powodował zbyt duże całkowite obciążenie procesora, co zaburzało pracę m.in. wątku odbioru danych z USRP. Z kolei śledzenie sygnałów GPS jest realizowane w czterech wątkach. Sygnały wykryte podczas akwizycji są kolejno rozdzielane pomiędzy poszczególne wątki śledzenia, tak aby zapewnić możliwie równomierne obciążenie procesora. Dzięki wprowadzeniu wielowątkowego wykonywania akwizycji i śledzenia sygnałów GPS, czas przetwarzania jednego segmentu danych skrócił się około trzykrotnie, względem przypadku przetwarzania sekwencyjnego.

5.4 Źródło sygnałów GPS

Realizacja badań pomiarowych systemu antyspoofingowego wymaga dysponowania generatorem sygnałów GPS, których parametry mogą być konfigurowalne przez operatora. Taki generator może stanowić źródło sygnałów fałszywych (spoofer), które są transmitowane przez pojedynczą antenę i docierają do odbiornika z tego samego kierunku.

Rysunek 5.8: Wektorowy generator sygnałów Rohde & Schwarz SMU200A

Jako spoofer w badaniach zastosowano wektorowy generator sygnałów SMU200A firmy Rohde & Schwarz [83], który został przedstawiony na Rys. 5.8. Generator ten wyposażono w opcję wytwarzania równocześnie maksymalnie ośmiu sygnałów GPS. Parametry tych sygnałów, jak również zawartości depesz nawigacyjnych, mogą zostać dowolnie skonfigurowane przez użytkownika. Między innymi, jest możliwe zadanie współrzędnych położenia i czasu, jakie powinien wskazać odbiornik GPS, na którego wejście są podane wytworzone sygnały. W takim przypadku, parametry i depesze sygnałów są generowane automatycznie, w oparciu o wczytany plik tekstowy z danymi almanachu w formacie YUMA. Treści depesz nawigacyjnych nie mają znaczenia dla funkcjonowania przyjętych metod antyspoofingowych. W badaniach użyto depesz stanowiących sekwencje składające się z samych zer logicznych.

Wyjście sygnałowe w.cz. generatora podłączono bezpośrednio do wejścia anteny nadawczej. Użycie dodatkowego wzmacniacza mocy nie było konieczne, gdyż moc wyjściowa generatora

jest w zupełności wystarczająca do zakłócenia odbioru sygnałów GPS w konfiguracji pomiarowej, gdzie długość trasy propagacji sygnału od spoofera do odbiornika nie przekracza kilkudziesięciu metrów.

Fałszywe sygnały nadawano z użyciem anteny o kierunkowej charakterystyce promieniowania w płaszczyźnie poziomej i pionowej. Miało to na celu ograniczenie ewentualnego oddziaływania sygnałów spoofera na inne pobliskie odbiorniki GPS, jak również ograniczenie efektu propagacji wielodrogowej.

Rozdział 6

Badania pomiarowe efektywności systemu antyspoofingowego

Tę część rozprawy poświęcono pomiarom parametrów, opracowanego przez autora, systemu antyspoofingowego, które zostały przeprowadzone z użyciem stanowiska badawczego, opisanego w poprzednim rozdziale. Na wstępie zostały przedstawione konfiguracje stanowiska, które były stosowane w różnych scenariuszach pomiarów. Konfiguracje różnią się między sobą m.in. sposobem doprowadzenia sygnałów fałszywych i prawdziwych do torów odbiorczych stanowiska.

W dalszej kolejności przedstawiono wyniki pomiarów odchylenia standardowego estymacji opóźnień fazowych oraz pomiarów prawdopodobieństwa detekcji spoofingu. Ich celem było zweryfikowanie wyników uzyskanych uprzednio na drodze symulacji.

Pozostała, najbardziej obszerna, część rozdziału dotyczy badań efektywności wykrywania i eliminacji spoofingu, w przypadkach odbioru od czterech do ośmiu sygnałów fałszywych. Dla tych pomiarów zostały zdefiniowane dodatkowe parametry jakościowe, umożliwiające ocenę pracy systemu w różnych warunkach.

6.1 Program badań pomiarowych

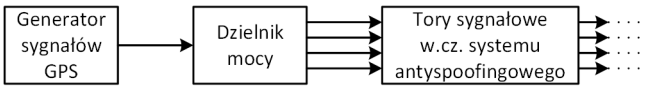
Zakres przeprowadzonych badań pomiarowych został podzielony na cztery etapy. W każdym z tych etapów zastosowano inną konfigurację stanowiska badawczego. Każda z konfiguracji była uzależniona od przyjętej charakterystyki kanału, przez który odbywa się transmisja sygnałów GPS. Zasadniczo można przyjąć, że pierwsza konfiguracja odpowiada uproszczonemu modelowi przyjętemu w badaniach symulacyjnych, natomiast każda kolejna jest coraz bardziej zbliżona do przypadku transmisji sygnałów w rzeczywistym kanale radiowym. Poniżej opisano poszczególne etapy badań pomiarowych, wraz odpowiadającymi im konfiguracjami stanowiska badawczego.

6.1.1 Etap I

Realizację badań pomiarowych rozpoczęto od zweryfikowania wyników uzyskanych w badaniach symulacyjnych, dotyczących wykrywania spoofingu GPS. Sprawdzono, czy, odchylenie standardowe błędu estymacji opóźnień fazowych, wyznaczanych przez opracowany prototyp, pokrywa się z krzywą opisaną wzorem (4.7). Następnie, zmierzono prawdopodobieństwo wykrycia spoofingu, przy wartościach progu detekcji zapisanych w Tab. 4.2.

Oba rodzaje pomiarów były przeprowadzone w warunkach zbliżonych do tych, które zostały przyjęte w symulacjach, tzn.

- brak wpływu sygnałów prawdziwych na transmisję sygnałów spoofera oraz
- kanał transmisyjny w którym sygnał jest zniekształcany wyłącznie przez oddziaływanie białego addytywnego szumu gaussowskiego.



Rysunek 6.1: Schemat blokowy konfiguracji pomiarowej I

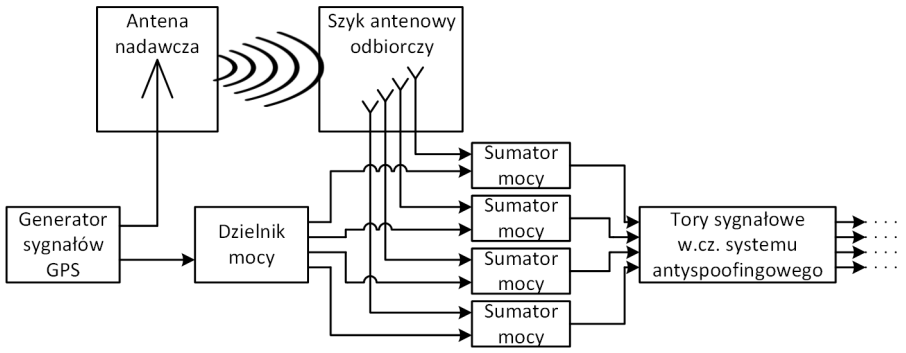
Aby zapewnić takie warunki transmisji, zastosowano konfigurację I stanowiska, której schemat przedstawia Rys. 6.1. Jest to podstawowy wariant stanowiska, w którym fałszywe sygnały GPS są doprowadzone przewodowo do wejść systemu antyspoofingowego. Sygnały z wyjścia generatora są rozdzielane w dzielniku mocy na cztery wyjścia, a każde z wyjść dzielnika jest połączone z wejściem odpowiedniego toru sygnałowego w.cz. Takie rozwiązanie umożliwia uniezależnienie wyników pomiarów od efektów związanych z transmisją w kanale bezprzewodowym, w tym m.in. propagacji wielodrogowej.

6.1.2 Etap II

Kolejnym etapem badań był pomiar tłumienia sygnałów spoofera w procesie filtracji przestrzennej. Należy tutaj zaznaczyć, że, w przypadku systemu GPS, nie jest możliwy bezpośredni pomiar tłumienia, np. przy użyciu metod analizy widmowej. Wynika to stąd, że, po pierwsze, w tym samym pasmie częstotliwości jest przesyłanych wiele sygnałów GPS, a po drugie, moc tych sygnałów w punkcie odbioru jest na tyle mała, że ich widmo nie jest widoczne na tle widma szumów. W związku z tym, dokonano przybliżonej oceny tłumienia na podstawie pomiaru wartości $\frac{C}{N_0}$ przed i po filtracji przestrzennej. Taka pośrednia metoda wiąże się jednak z istotnym ograniczeniem. Umożliwia ona pomiar tłumienia wynoszącego co najwyżej tyle, co stosunek mocy sygnału przed filtracją do mocy odpowiadającej czułości odbiornika GPS. Przykładowo, jeśli odbierany sygnał ma $\frac{C}{N_0}$ równe 50 dBHz, a do poprawnego odbioru sygnału jest wymagane $\frac{C}{N_0}$ na poziome co najmniej 30 dBHz, to jest możliwy pomiar tłumienia nie większego niż 20 dB. Nawet jeśli filtracja przestrzenna stłumi sygnał o więcej niż 20 dB, wyznaczone $\frac{C}{N_0}$ sygnału wyjściowego nie będzie mniejsze niż 30 dBHz.

Równocześnie z pomiarem zmiany $\frac{C}{N_0}$ sygnałów fałszywych, w etapie II określono wpływ filtracji przestrzennej na wartość $\frac{C}{N_0}$ prawdziwego sygnału GPS. Na tym etapie badań, rolę sygnału prawdziwego pełnił sygnał wytworzony lokalnie w generatorze wektorowym, podobnie jak sygnały fałszywe. Zastosowano tu konfigurację II stanowiska badawczego, której schemat został przedstawiony na Rys. 6.2. W tym przypadku fałszywe sygnały są, podobnie jak w konfiguracji I, przesyłane przewodowo do systemu antyspoofingowego. Generator wytwarza również pojedyn-

czy sygnał GPS, z innym ciągiem C/A niż ciągi sygnałów fałszywych. Ten jeden sygnał pełni rolę testowego sygnału prawdziwego. Jest on transmitowany bezprzewodowo poprzez antenę nadawczą, podłączoną do drugiego wyjścia w.cz. generatora. Odbiór tego sygnału odbywa się z użyciem szyku antenowego. Opóźnienia fazowe fal nośnych sygnału prawdziwego i sygnałów fałszywych różnią się. Sygnał prawdziwy z wyjścia każdego elementu antenowego jest sumowany z sygnałami fałszywymi z odpowiedniego wyjścia dzielnika mocy. Takie kombinacje sygnałów trafiają na wejścia torów odbiorczych w.cz. Zarówno antena nadawcza, jak i szyk odbiorczy, znajdują się wewnątrz budynku i jest zachowana pomiędzy nimi bezpośrednia widoczność (LoS).



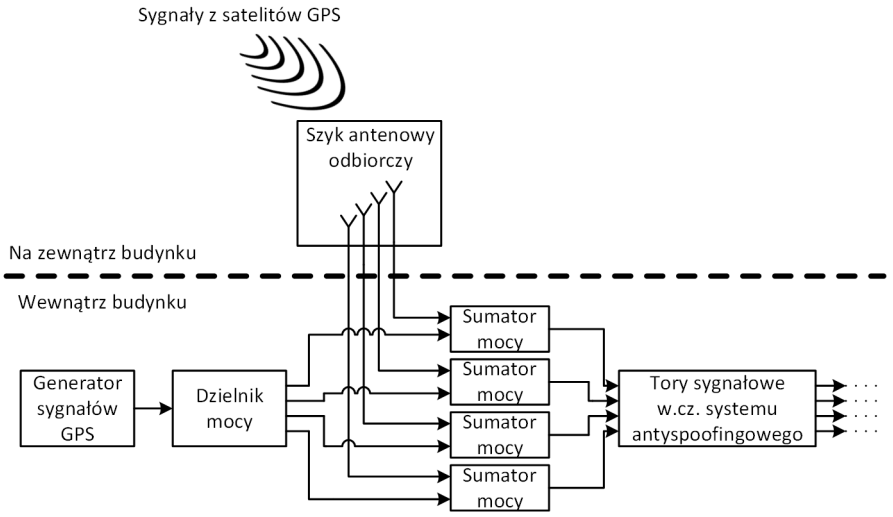
Rysunek 6.2: Schemat blokowy konfiguracji pomiarowej II

Każdy dwóch z torów generatora wektorowego może niezależnie wytwarzać maksymalnie cztery sygnały GPS. Z uwagi na użycie jednego z tych torów do wytworzenia sygnału prawdziwego, w tej konfiguracji jest więc możliwe nadawanie maksymalnie czterech fałszywych sygnałów GPS.

Użycie takiej konfiguracji pozwala na przebadanie scenariusza, w którym do odbiornika docierają sygnały fałszywe oraz sygnał prawdziwy, przy czym ten ostatni nadchodzi z innego, niezmiennego w czasie, kierunku. Zaletą takiego rozwiązania jest możliwość dowolnego kontrolowania mocy nadawanego sygnału prawdziwego.

6.1.3 Etap III

Pomiary uwzględnione w poprzednim etapie zakładają odbiór pojedynczego sygnału prawdziwego z jednego kierunku. W warunkach rzeczywistych do odbiornika dociera wiele sygnałów prawdziwych o różnych kierunkach nadejścia. Taka sytuacja nie jest możliwa do odtworzenia w konfiguracji II stanowiska. Dlatego też, w kolejnym - trzecim etapie badań, sygnałami prawdziwymi były rzeczywiste sygnały odbierane z satelitów systemu GPS. Aby zapewnić możliwość ich odbioru, zestawiono konfigurację III stanowiska pomiarowego, której schemat zobrazowano na Rys. 6.3.



Rysunek 6.3: Schemat blokowy konfiguracji pomiarowej III

Różnica pomiędzy tą konfiguracja a konfiguracją II polega na tym, że generator nie jest używany do wytwarzania sygnału prawdziwego. Podobnie jak w konfiguracji I, jest wytwarzanych od czterech do ośmiu sygnałów fałszywych, przy użyciu obu torów sygnałowych generatora. Z kolei odbiorczy szyk antenowy jest umieszczony na zewnątrz budynku, tak aby docierały do niego prawdziwe sygnały pochodzące z satelitów GPS.

Takie rozwiązanie umożliwia ocenę efektywności przyjętych metod antyspoofingowych w obecności rzeczywistych sygnałów GPS, jednakże bez uwzględnienia efektów w kanale bez-

przewodowym pomiędzy spooferem a odbiornikiem GPS.

Wyniki pomiarów uzyskanych na tym, jak również na kolejnym, IV etapie badań, umożliwiają dokonanie analizy:

- skuteczności i poprawności wykrywania spoofingu,
- zmian wartości $\frac{C}{N_0}$ sygnałów fałszywych i prawdziwych, spowodowanych filtracją przestrzenną,
- rozkładu liczby sygnałów prawdziwych i fałszywych przed i po eliminacji spoofingu.

Charakter takiej analizy jest różny od tej, która została przeprowadzona na podstawie wyników badań symulacyjnych. Ta odmienność wynika ze specyfiki badań pomiarowych, m.in. z ograniczonego przedziału czasu wykonywania pomiarów (pomiary realizowane tylko w porze dziennej) oraz z ustalonej lokalizacji stanowiska badawczego. Zmiana podejścia do oceny efektywności systemu antyspoofingowego spowodowała konieczność ustalenia nowego zbioru parametrów jakościowych. Definicje tych parametrów zostały przedstawione w Tab. 6.1 i 6.2.

Tabela 6.1: Parametry oceny detekcji spoofingu w etapach III i IV badań pomiarowych

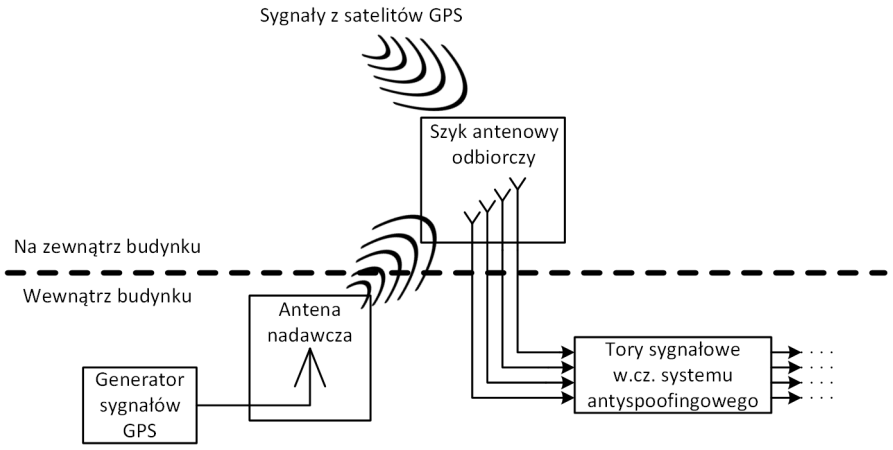
Symbol	Opis
N_{det}	Całkowita liczba detekcji spoofingu w serii pomiarowej
$N_{det\ OK}$	Liczba detekcji spoofingu z poprawnym określeniem numerów fałszywych sygnałów
$N_{det\ \subset S_{spoof}}$	Liczba detekcji spoofingu z niewykryciem jednego lub więcej fałszywych sygnałów
$N_{det\ \notin S_{spoof}}$	Liczba detekcji spoofingu z uznaniem co najmniej jednego sygnału prawdziwego za fałszywy
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	Liczba detekcji spoofingu z niewykryciem jednego lub więcej fałszywych sygnałów i uznaniem co najmniej jednego sygnału prawdziwego za fałszywy
$P_{sygn\ [\sim det \mid \in S_{spoof}]}$	Rozkład liczby niewykrytych sygnałów fałszywych
$P_{sygn\ [\in S_{spoof} \mid \notin S_{spoof}]}$	Rozkład liczby prawdziwych sygnałów uznanych za fałszywe

Tabela 6.2: Parametry oceny eliminacji spoofingu w etapach III i IV badań pomiarowych

Symbol	Opis
$\overline{\frac{C}{N_0}}_{\in S_{spoof}}$	Średnia wartość $\frac{C}{N_0}$ sygnałów fałszywych przed filtracją przestrzenną
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}}$	Średnia wartość $\frac{C}{N_0}$ sygnałów prawdziwych przed filtracją przestrzenną
$P_{\notin S_{spoof}}$	Rozkład liczby sygnałów prawdziwych przed filtracją przestrzenną
$\overline{\frac{C}{N_0}}_{\in S_{spoof}\ filtr}$	Średnia wartość $\frac{C}{N_0}$ sygnałów fałszywych po filtracji przestrzennej
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}\ filtr}$	Średnia wartość $\frac{C}{N_0}$ sygnałów prawdziwych po filtracji przestrzennej
$P_{\notin S_{spoof}\ filtr}$	Rozkład liczby sygnałów prawdziwych po filtracji przestrzennej

6.1.4 Etap IV

Ostatni etap badań pomiarowych miał na celu umożliwienie oceny funkcjonowania systemu antyspoofingowego w warunkach rzeczywistych, gdy zarówno sygnały fałszywe, jak i prawdziwe, są transmitowane bezprzewodowo i odbierane z użyciem szyku antenowego.



Rysunek 6.4: Schemat blokowy konfiguracji pomiarowej IV

Przyjęta, w tym przypadku, konfiguracja IV stanowiska pomiarowego różni się od poprzedniej tym, że wyjście w.cz. generatora, wytwarzającego maksymalnie 8 sygnałów GPS, jest połączone bezpośrednio z kierunkową anteną nadawczą. Schemat konfiguracji IV przedstawiono na Rys. 6.4.

W tej konfiguracji jest uwzględnione oddziaływanie kanału radiowego na transmisję sygnałów fałszywych. Efekty tego oddziaływania są uzależnione od charakteru środowiska propagacji oraz od wzajemnego położenia i orientacji anteny nadawczej i odbiorczego szyku antenowego.

Zestaw parametrów oceny jakościowej był w tym etapie badań identyczny z tym, który zastosowano w etapie III.

Poszczególne serie pomiarów wykonanych w etapach III i IV są identyfikowane poprzez unikatowe oznaczenia, tzw. scenariusze pomiarowe. Nazwy scenariuszy mają następujący format: "numer konfiguracji stanowiska"_"zestaw parametrów"_"liczba fałszywych sygnałów". Przez różne parametry pomiaru są rozumiane, np. różne charaktery środowiska propagacji, różne warianty parametrów procedur detekcji lub eliminacji spoofingu itp. Pojęcie zestawu parametrów obejmuje m.in.: charakter środowiska propagacji, parametry procedur detekcji i eliminacji spoofingu itp. Przykładowo, nazwa scenariusza pomiarowego w konfiguracji III, przy transmisji czterech fałszywych sygnałów i zestawie parametrów oznaczonym literą A, jest zapisana jako III_A_4.

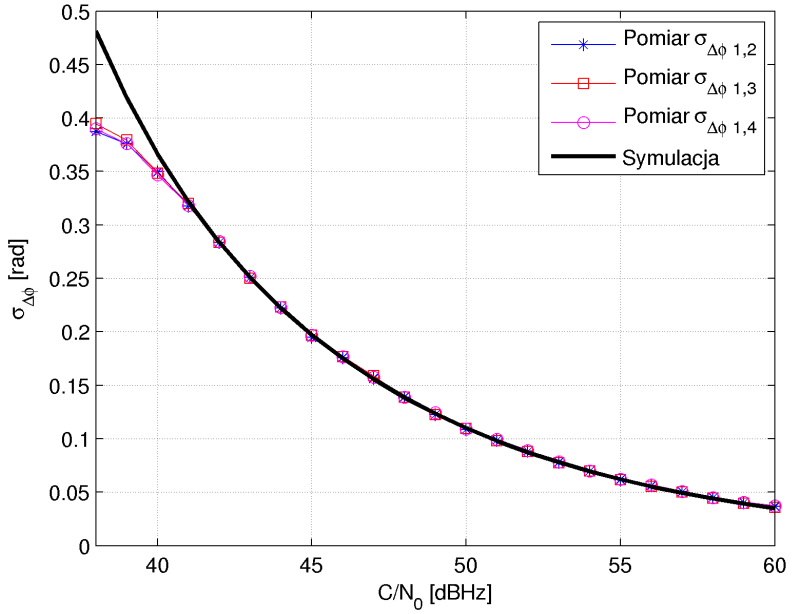
6.2 Analiza wyników I etapu badań

Jak wspomniano w poprzednim punkcie, w pierwszym etapie badań dokonano pomiarowej weryfikacji następujących charakterystyk wyznaczonych w badaniach symulacyjnych: zależności odchylenia standardowego estymacji opóźnień fazowych od wartości $\frac{C}{N_0}$ oraz zależności prawdopodobieństwa detekcji spoofingu od wartości $\frac{C}{N_0}$ i liczby odbieranych sygnałów fałszywych.

6.2.1 Pomiar odchylenia standardowego estymacji opóźnień fazowych

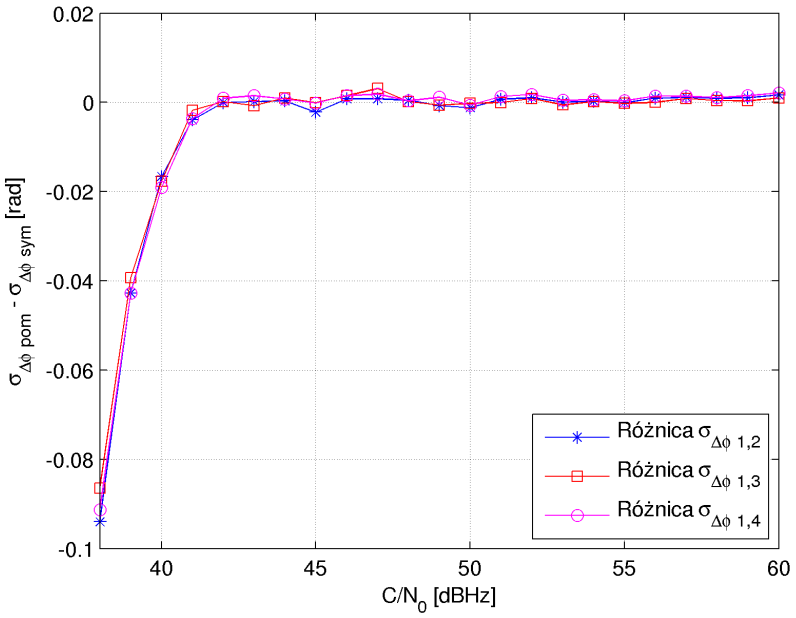
Badania rozpoczęto od określenia wartości odchylenia standardowego $\sigma_{\Delta\phi}$ estymacji opóźnień fazowych. Badania przeprowadzono w konfiguracji I stanowiska. Uzyskane wyniki zapre-

zentowano na Rys. 6.5. Krzywa koloru czarnego reprezentuje wyniki otrzymane w badaniach symulacyjnych, natomiast pozostałe trzy wykresy to uśrednione wartości $\sigma_{\Delta\phi}$ opóźnień fazowych zmierzonych w trzech parach elementów antenowych.



Rysunek 6.5: Zmierzone odchylenia standardowe błędu estymacji opóźnień fazowych

Na Rys. 6.6 przedstawiono różnicę pomiędzy wynikami pomiarów a wynikami symulacji. Dla wartości $\frac{C}{N_0}$ większych niż 41 dBHz wyniki są niemal identyczne. Z kolei przy mniejszych wartościach stosunku $\frac{C}{N_0}$ zmierzone odchylenie standardowe jest nieco mniejsze niż wynika to z symulacji. Różnica ta może być spowodowana tym, że w badaniach symulacyjnych rozpatrywano odbiór pojedynczego sygnału GPS w obecności idealnego szumu AWGN, którego realizacje na wejściach poszczególnych torów odbiorczych są wzajemnie nieskorelowane. W warunkach rzeczywistych warunek całkowitego braku korelacji szumów w różnych torach nie jest spełniony. Przykładem może być szum fazy oscylatorów lokalnych w urządzeniach USRP, które są sterowane przez wspólny wzorzec częstotliwości 10 MHz. Występowanie niezerowej korelacji szumów może prowadzić do zmniejszenia wariancji (a tym samym zmniejszenia odchylenia standardowego) błędu estymacji opóźnień fazowych.

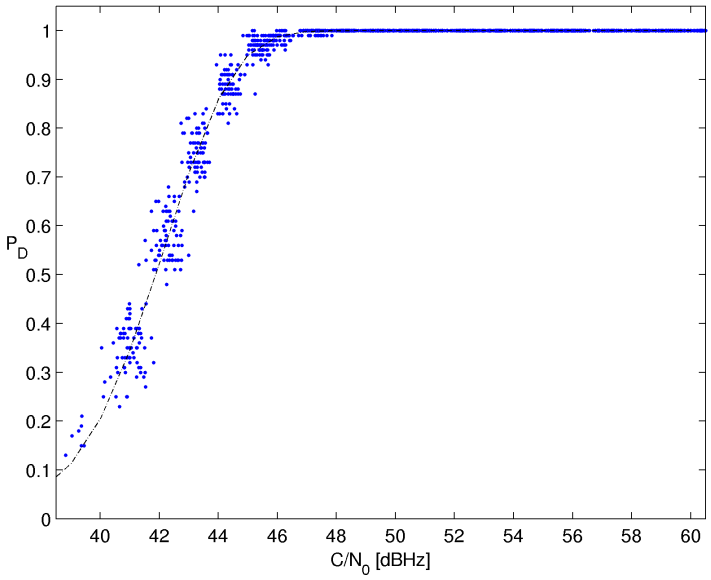


Rysunek 6.6: Różnice pomiędzy wynikami pomiarów i symulacji odchylenia standardowego błędu esytymacji opóźnień fazowych

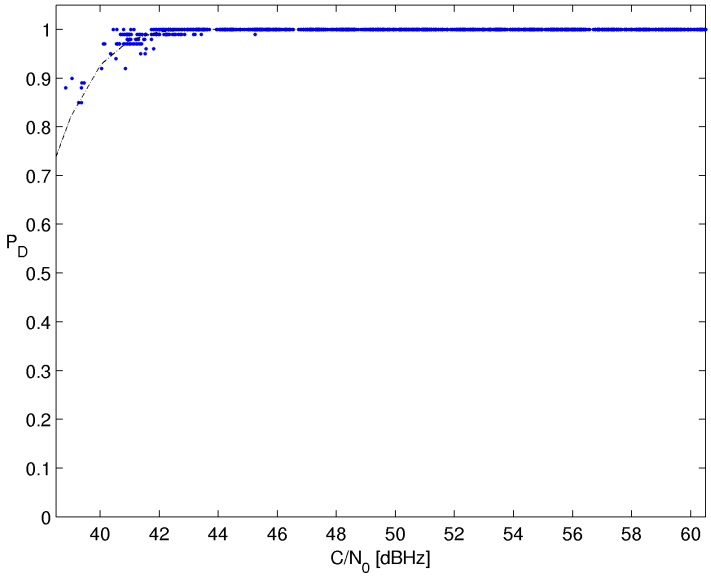
6.2.2 Pomiar prawdopodobieństwa detekcji spoofingu

Właściwa ocena efektywności systemu antyspoofingowego wymaga pomiaru parametrów związanych z wykrywaniem i eliminacją spoofingu. W pierwszej kolejności dokonano pomiarów prawdopodobieństwa detekcji spoofingu. Pomiary te przeprowadzono w konfiguracji I stanowiska badawczego. Analizowany zakres wartości $\frac{C}{N_0}$ był taki sam jak w przypadku pomiaru odchylenia standardowego błędu estymacji opóźnień fazowych. W trakcie całej serii pomiarowej nadawano osiem sygnałów GPS i określano wartości prawdopodobieństw detekcji spoofingu dla przypadków odbioru od 4 do 8 sygnałów fałszywych. Pojedynczy pomiar prawdopodobieństwa był realizowany w oparciu o jeden segment próbek sygnału o długości 250 ms.

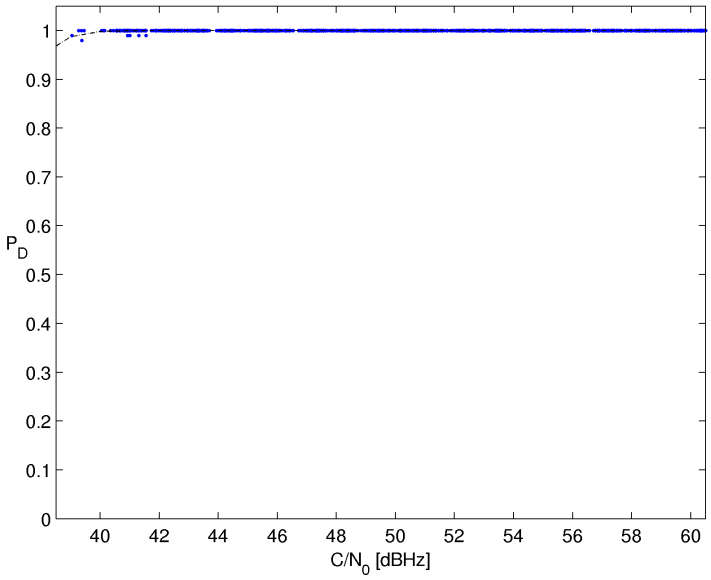
Na rysunkach: od 6.7 do 6.11 przedstawiono uzyskane wyniki pomiarów prawdopodobieństwa detekcji spoofingu. Czarna linia przerywana reprezentuje charakterystykę prawdopodobieństwa detekcji w funkcji $\frac{C}{N_0}$, określoną na podstawie symulacji. Natomiast każda z niebieskich kropek przedstawia wynik pojedynczego pomiaru prawdopodobieństwa.



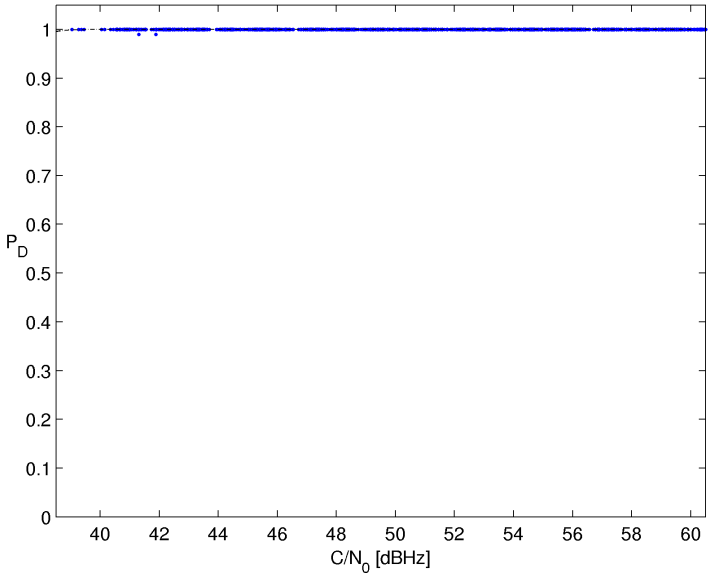
Rysunek 6.7: Zmierzone prawdopodobieństwo detekcji spoofingu przy 4 fałszywych sygnałach



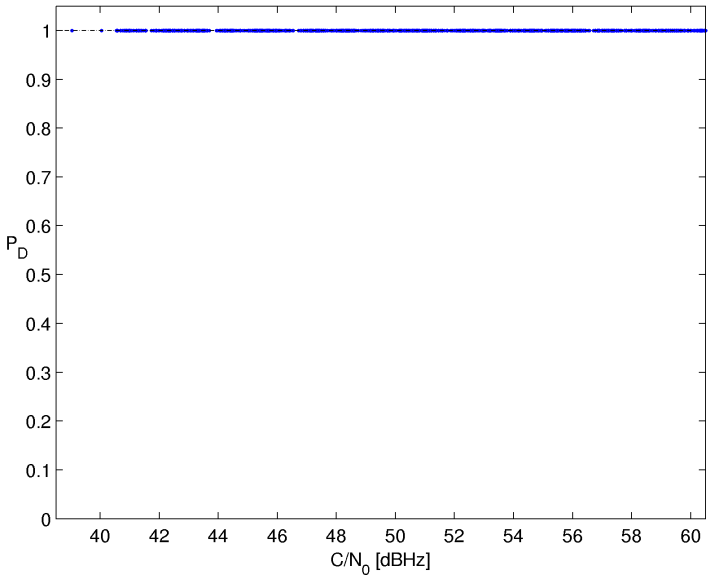
Rysunek 6.8: Zmierzone prawdopodobieństwo detekcji spoofingu przy 5 fałszywych sygnałach



Rysunek 6.9: Zmierzone prawdopodobieństwo detekcji spoofingu przy 6 fałszywych sygnałach



Rysunek 6.10: Zmierzone prawdopodobieństwo detekcji spoofingu przy 7 fałszywych sygnałach



Rysunek 6.11: Zmierzone prawdopodobieństwo detekcji spoofingu przy 8 fałszywych sygnałach

W ramach każdej serii dokonano w sumie 1500 pomiarów. Wartość $\frac{C}{N_0}$ związana z każdym pomiarem stanowi średnią arytmetyczną wartości $\frac{C}{N_0}$ wyznaczonych dla poszczególnych sygnałów spoofera.

Na wszystkich wykresach można zauważyć, że wyniki uzyskane w trakcie pomiarów są zgodne krzywą symulacyjną. Dla wartości $\frac{C}{N_0}$, dla których prawdopodobieństwo detekcji spoofingu jest mniejsze od 1, wyniki pomiarów są skoncentrowane wokół tej krzywej. Charakterystyczna "nieciągłość" wyników pomiarów, widoczna zwłaszcza na Rys. 6.7, jest spowodowana tym, że moc sygnałów GPS była zmieniana w trakcie serii pomiarowej z krokiem co 1 dB. Dla przypadków wykrycia sześciu i więcej fałszywych sygnałów, prawdopodobieństwo detekcji całym w rozpatrywanym zakresie $\frac{C}{N_0}$ jest bliskie jedności, a wyniki pomiarów pokrywają się z wynikami symulacji. Wraz ze wzrostem liczby fałszywych sygnałów, dla której jest wyznaczane prawdopodobieństwo spoofingu, można zaobserwować zmniejszanie się liczby pomiarów o najmniejszych wartościach $\frac{C}{N_0}$. Wynika to stąd, że, przy małych wartościach stosunku $\frac{C}{N_0}$, procedura akwizycji nie zawsze wykrywała wszystkie spośród ośmiu nadawanych fałszywych sygnałów GPS.

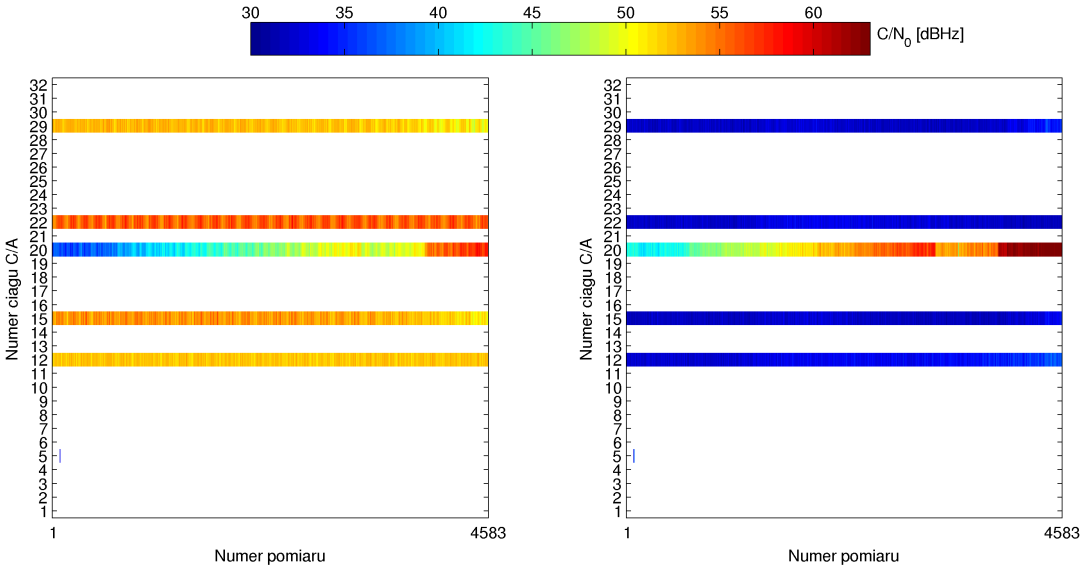
W związku z tym, w przypadku wykrycia np. jedynie 6 sygnałów, nie było możliwości wyznaczenia prawdopodobieństwa spoofingu dla 7 i 8 sygnałów.

6.3 Analiza wyników II etapu badań

Kolejny etap pomiarów efektywności systemu antyspoofingowego był realizowany w konfiguracji II stanowiska pomiarowego. Miał on na celu zbadanie zmian jakości odbieranych sygnałów GPS, spowodowanych filtracją przestrzenną, z użyciem której jest realizowana eliminacja spoofingu.

W serii pomiarowej, której wyniki są prezentowane, nadawano cztery sygnały fałszywe o numerach ciągów C/A: 12, 15, 22 i 29 oraz jeden sygnał, pełniący rolę sygnału prawdziwego, o numerze ciągu C/A 20. Moc sygnałów fałszywych była utrzymywana na stałym poziomie, przy którym wartość stosunku $\frac{C}{N_0}$ dla tych sygnałów wynosiła ok. 55 dBHz. Z kolei moc odbieranego sygnału prawdziwego na początku serii pomiarowej była o 20 dB mniejsza niż moce odbieranych sygnałów fałszywych i była w trakcie serii pomiarowej stopniowo zwiększana do wartości przekraczającej moc sygnałów fałszywych o 3 dB. W trakcie serii dokonano 4583 pomiarów.

Przed omówieniem uzyskanych wyników, konieczne jest objaśnienie, przyjętego w dalszej części rozprawy, sposobu graficznej reprezentacji pomierzonych wartości stosunków $\frac{C}{N_0}$. Zastosowano tu tzw. wykres pseudokolorowy, zwany również wykresem szachownicowym. Oś pionowa takiego wykresu określa w tym przypadku numer ciągu C/A sygnału GPS, a oś pozioma numer pomiaru w ramach jednej serii. Wartość $\frac{C}{N_0}$ jest reprezentowana przez kolor każdego pola odpowiadającego danemu numerowi ciągu C/A i numerowi pomiaru. Zgodnie z przyjętą paletą odwzorowania kolorów, wartości $\frac{C}{N_0}$ równej 30 dBHz odpowiada kolor ciemnoniebieski, a wartości 63 dBHz kolor ciemnoczerwony. Wartości pośrednie pomiędzy 30 a 63 są reprezentowane przez odcienie: błękitnego, zielonego, żółtego i pomarańczowego. W przypadku, gdy sygnał z danym ciągiem C/A nie jest wykryty w fazie akwizycji, pole pozostaje białe. Zastosowanie takiego rodzaju graficznej reprezentacji wyników poprawia jej czytelność. Przebiegi $\frac{C}{N_0}$ dla poszczególnych sygnałów można analizować niezależnie, co jest szczególnie istotne, gdy liczba odbieranych sygnałów GPS jest duża.

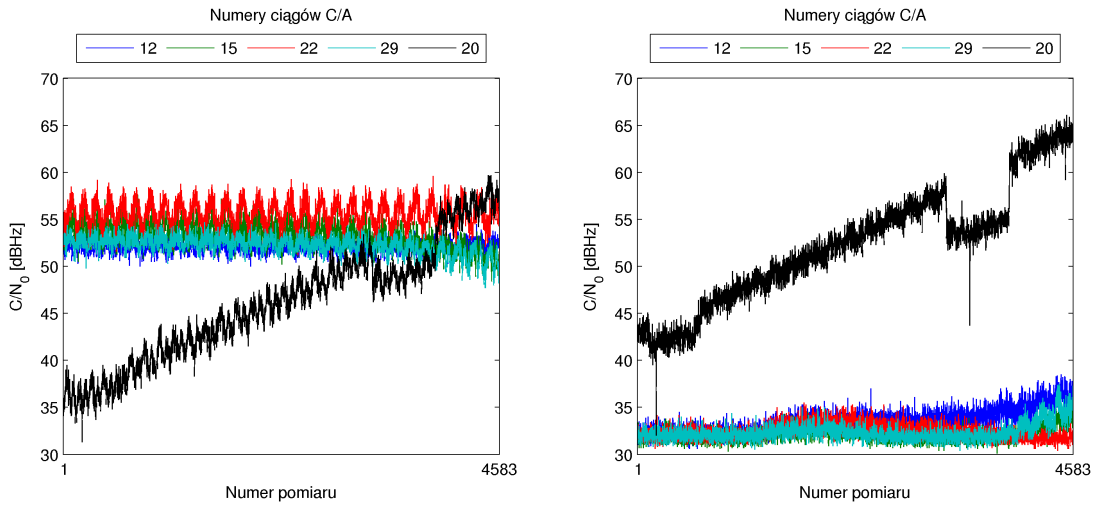


Rysunek 6.12: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (konfiguracja II)

Na Rys. 6.12 przedstawiono wykresy pseudokolorowe wartości $\frac{C}{N_0}$ dla poszczególnych sygnałów GPS przed eliminacją spoofingu (po lewej) i po tej eliminacji (po prawej). Wyniki te zaprezentowano również, w postaci wykresów liniowych $\frac{C}{N_0}$ w funkcji numeru pomiaru, na Rys. 6.13. Widać wyraźnie, że proces filtracji przestrzennej spowodował spadek wartości $\frac{C}{N_0}$ sygnałów fałszywych do poziomu pomiędzy 30 dBHz a 35 dBHz. W praktyce oznacza to, że te sygnały zostały całkowicie wyeliminowane i nie zostałyby one ponownie wykryte w fazie akwizycji. **Uwaga: W pozostałej części rozprawy, na wykresach pseudokolorowych nie są uwzględniane wartości $\frac{C}{N_0}$ sygnałów niewykrywanych w procesie akwizycji. W powyższym przypadku byłby to sygnał o numerze ciągu 20 przed filtracją przestrzenną, na początku serii pomiarowej oraz sygnały o numerach 12, 15, 22 i 29 po filtracji przestrzennej, w całej serii.**

W przypadku sygnału prawdziwego, jest zauważalny wzrost jego wartości $\frac{C}{N_0}$ o ok. 7 dB w stosunku do wartości przed filtracją przestrzenną. W przebiegu $\frac{C}{N_0}$ sygnału prawdziwego można zauważyć przedziały czasu, w których wystąpił skokowy spadek wartości. W przypadku sygnałów fałszywych taki spadek nie został zaobserwowany. Biorąc pod uwagę fakt, że sygnał

prawdziwy był transmitowany radiowo, a sygnały fałszywe przewodowo, można przypuszczać że spadek $\frac{C}{N_0}$ był spowodowany tymczasowymi zmianami właściwości kanału radiowego, np. wystąpieniem interferencji w pasmie systemu GPS.



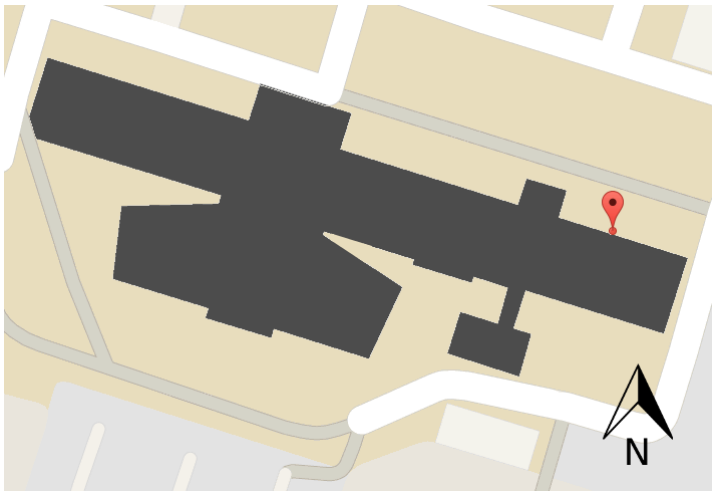
Rysunek 6.13: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (konfiguracja II)

Uzyskane wyniki wskazują na poprawne działanie systemu antyspoofingowego w przypadku odbioru czterech sygnałów fałszywych o stosunkowo dużej mocy. Należy jednak mieć na względzie to, że przyjęta tu konfiguracja pomiarowa umożliwia przeprowadzenie badań jedynie w warunkach laboratoryjnych, które znacząco odbiegają od tych, które mogą wystąpić w rzeczywistym przypadku spoofingu.

6.4 Analiza wyników III etapu badań

W tym i w następnym punkcie niniejszego rozdziału przedstawiono wyniki pomiarów, których analiza umożliwia dokonanie całościowej ewaluacji proponowanego systemu antyspoofingowego. W trakcie każdego pomiaru określano m.in. liczbę i numery prawdziwych i fałszywych sygnałów przed i po eliminacji spoofingu wraz z wartościami $\frac{C}{N_0}$ tych sygnałów. Taki zbiór informacji jest wystarczający do oceny poprawności działania algorytmu detekcji spoofingu, jak również do oceny efektywności filtracji przestrzennej.

Aby dokonać pełnej oceny wykrywania i eliminacji spoofingu, dla pomiarów przeprowadzanych w konfiguracjach III i IV, użyto parametrów jakościowych, zdefiniowanych w tabelach 6.1 i 6.2.



Rysunek 6.14: Położenie szyku antenowego (czerwona pinezka) w odniesieniu do budynku WETI PG (ciemnoszary kontur)

W trzecim etapie badań, mając na celu przeprowadzenie pomiarów w warunkach bardziej zbliżonych do rzeczywistych, zastąpiono, wytwarzany w generatorze, pojedynczy sygnał prawdziwy, wieloma sygnałami odbieranymi z satelitów GPS (konfiguracja pomiarowa III). Szyk antenowy umieszczono za oknem laboratorium, znajdującego się na czwartym piętrze budynku Wydziału Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej (WETI PG). Zgrubne położenie szyku antenowego zostało zaprezentowane na Rys. 6.14 [30].

Przed przystąpieniem do oceny efektywności przeciwdziałania spoofingowi w tej konfiguracji pomiarowej, określono nominalną widoczność satelitów GPS w punkcie pomiarowym.

6.4.1 Widoczność satelitów GPS w punkcie pomiarowym

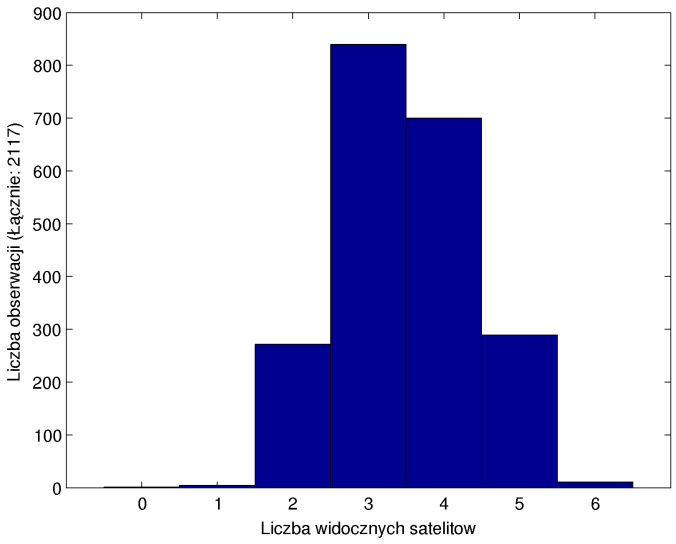
W tym miejscu warto przypomnieć, że jednym z głównych zadań sytemu antyspoofingowego jest zapewnienie możliwości odbioru prawdziwych sygnałów GPS w obecności spoofingu.

Liczba i jakość sygnałów odbieranych z satelitów powinna być możliwie bliska tej, jaka jest obserwowana w przypadku braku spoofingu. Parametry te są uzależnione od umiejscowienia anteny odbiorczej. Aby określić wartości referencyjne dla działania systemu antyspoofingowego, obserwowano widoczność satelitów w punkcie pomiarowym przy braku transmisji sygnałów spoofera.

Czas obserwacji wynosił 5 godzin i 30 minut. W tym czasie procedura akwizycji sygnałów GPS została wykonana 2117 razy. W Tab. 6.3 przedstawiono bezwzględne liczby oraz udział procentowy akwizycji, w których wykryto określoną liczbę sygnałów GPS z satelitów. Rys. 6.15 prezentuje histogram wyników obserwacji.

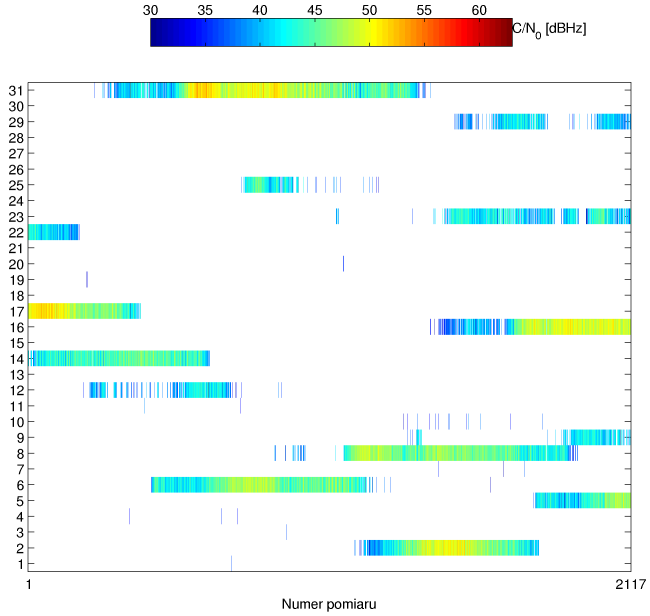
Tabela 6.3: Rozkład liczby satelitów GPS widocznych w punkcie pomiarowym

Liczba satelitów	0	1	2	3	4	5	6
Liczba obserwacji (wszystkich: 2117)	1	4	272	840	700	289	11
% obserwacji	0,05	0,19	12,85	39,68	33,06	13,65	0,52



Rysunek 6.15: Histogram liczby satelitów GPS widocznych w punkcie pomiarowym

Maksymalna liczba prawdziwych sygnałów GPS, którą odebrano w czasie serii pomiarowej, to sześć. Najczęściej odbierano trzy lub cztery sygnały. Tylko w jednym przypadku nie wykryto żadnego z nich. W warunkach pełnej widoczności nieba, odbiornik GPS może odbierać równocześnie nawet powyżej dziesięciu sygnałów. W przeprowadzonych obserwacjach ta liczba jest mniejsza, z uwagi na to, że widoczność satelitów w rozpatrywanym punkcie pomiarowym była znacząco ograniczona poprzez przeszkodę w postaci bryły budynku WETI PG. Okna laboratorium wychodzą na stronę północną, a budynek zasłania całą południową część nieba, z której zwykle dociera większość sygnałów GPS.



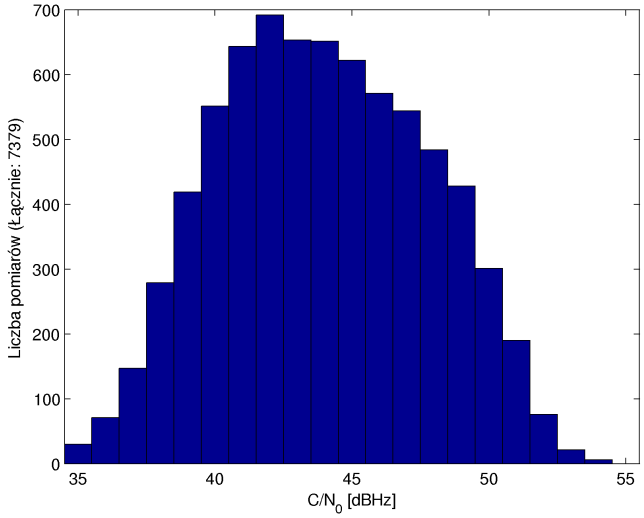
Rysunek 6.16: Wartości $\frac{C}{N_0}$ prawdziwych sygnałów GPS odbieranych w punkcie pomiarowym

Na Rys. 6.16 przedstawiono wykres pseudokolorowy zmierzonych wartości $\frac{C}{N_0}$ sygnałów odbieranych z satelitów. Z kolei Tab. 6.4 ukazuje empiryczny rozkład prawdopodobieństwa wystąpienia wartości $\frac{C}{N_0}$ z przedziału $\widehat{\frac{C}{N_0}} - 0,5dB \leqslant \frac{C}{N_0} < \widehat{\frac{C}{N_0}} + 0,5dB$, gdzie $\widehat{\frac{C}{N_0}}$ jest całkowitą wartością $\frac{C}{N_0}$ z zakresu od 35 dBHz do 54 dBHz. Rys. 6.17 przedstawia histogram zmierzonych wartości $\frac{C}{N_0}$. W trakcie serii pomiarowej nie odebrano sygnałów o $\frac{C}{N_0}$ większym niż 54,5 dBHz. Najczęściej odbierano sygnały o wartości tego stosunku równej ok. 42 dBHz.

Tabela 6.4: Rozkład zmierzonych wartości stosunku $\frac{C}{N_0}$ prawdziwych sygnałów GPS

$\frac{C}{N_0}$	Liczba pomiarów	% pomiarów	$\frac{C}{N_0}$	Liczba pomiarów	% pomiarów
35	30	0,41	45	622	8,43
36	71	0,96	46	571	7,74
37	147	1,99	47	544	7,37
38	279	3,78	48	484	6,56
39	419	5,68	49	428	5,80
40	551	7,47	50	301	4,08
41	643	8,71	51	190	2,58
42	692	9,38	52	76	1,03
43	653	8,85	53	21	0,28
44	651	8,82	54	6	0,08

Rysunek histogramu wskazuje, że rozkład jest asymetryczny, z ujemną skośnością. Wartość średnia ze wszystkich pomiarów $\frac{C}{N_0}$ wynosi ok. 44 dBHz. Zakres zmienności zmierzonych wartości jest zgodny z oczekiwaniami i nie wykracza poza, przyjęty w symulacjach, przedział od 35 dBHz do 60 dBHz.

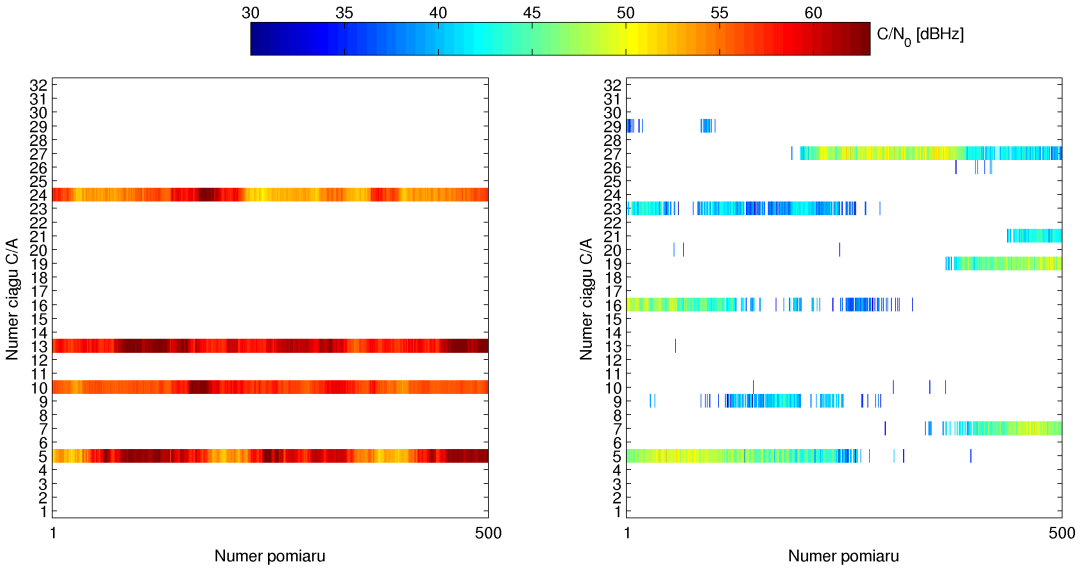


Rysunek 6.17: Histogram wartości $\frac{C}{N_0}$ prawdziwych sygnałów GPS

6.4.2 Efektywność procedur antyspoofingowych - transmisja przewodowa

Po określeniu widoczności satelitów GPS w miejscu obserwacji, przystąpiono do realizacji właściwych pomiarów w konfiguracji III, tym razem z uwzględnieniem sygnałów spoofera. Moc odbieranych sygnałów fałszywych była znacznie większa niż sygnałów prawdziwych, co sprawiło, że te ostatnie, w zdecydowanej większości przypadków, nie były wykrywane podczas pierwszej akwizycji (tzn. akwizycji wykonywanej przed eliminacją spoofingu). Nadawanie ze stosunkowo dużą mocą miało na celu odzwierciedlenie takich warunków spoofingu, gdzie przewaga mocy sygnałów spoofera całkowicie uniemożliwia odbiór sygnałów z satelitów GPS.

Rozpoczęto od scenariusza, w którym nadawano cztery sygnały fałszywe, których widmo było rozpraszane ciągami C/A o numerach: 5, 10, 13 i 24. Na wykresie pseudokolorowym wartości $\frac{C}{N_0}$ przed i po eliminacji (Rys. 6.18) widać, że sygnały 10, 13 i 24 zostały wyeliminowane. Sygnał 5 był obecny również po filtracji do ok. połowy czasu trwania serii pomiarowej. Jednakże nie był to już sygnał fałszywy, lecz prawdziwy, rozpraszany tym samym ciągiem pseudolosowym. Odmienność tych sygnałów stwierdzono na podstawie analizy chwil rozpoczęcia ciągu C/A oraz postaci depesz nawigacyjnych modulujących oba sygnały.



Rysunek 6.18: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz III_A_4)

Tabela 6.5: Parametry jakościowe detekcji spoofingu w scenariuszu III_A_4

	N_{wyst}	Udział
N_{det}	500	100,0%
$N_{det\ OK}$	500	100,0%
$N_{det\ \subset S_{spoof}}$	0	0,0%
$N_{det\ \notin S_{spoof}}$	0	0,0%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	—	—
6	—	—
7	—	—
8	—	—

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

Tabela 6.6: Parametry jakościowe eliminacji spoofingu w scenariuszu III_A_4

$\overline{\frac{C}{N_0}}_{\in S_{spoof}}$	57,3 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}}$	32,7 dBHz
$\overline{\frac{C}{N_0}}_{\in S_{spoof}\ filtr}$	31,9 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}\ filtr}$	44,1 dBHz

$P_{\notin S_{spoof}}$

N_{sygn}	N_{wyst}	Udział
0	500	100,0%
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

$P_{\notin S_{spoof}\ filtr}$

N_{sygn}	N_{wyst}	Udział
0	0	0,0%
1	61	12,2%
2	86	17,2%
3	211	42,2%
4	136	27,2%
5	6	1,2%
6	0	0,0%

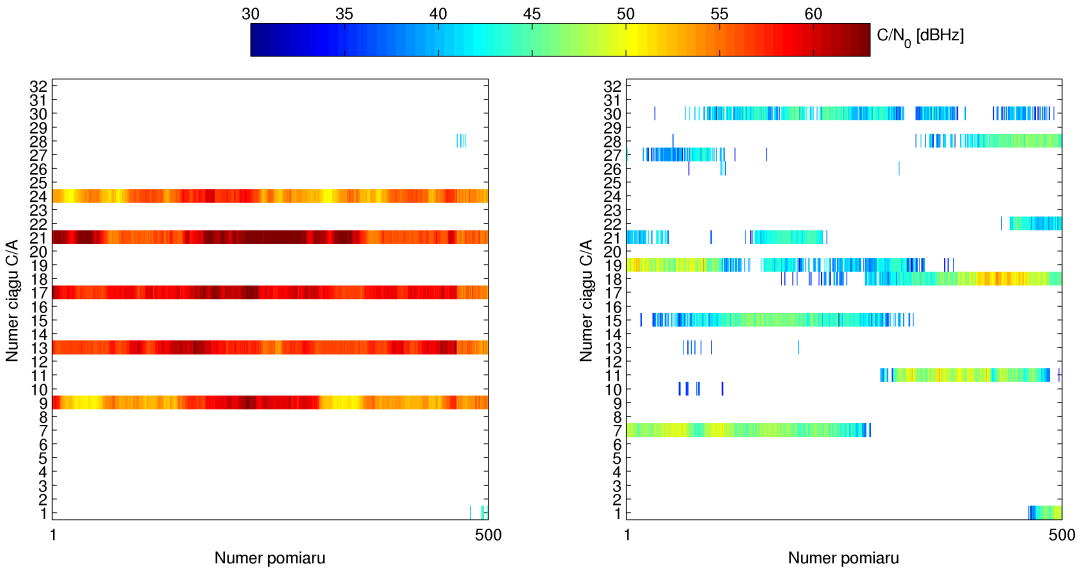
Tab. 6.5 zawiera wartości parametrów związanych z detekcją spoofingu w scenariuszu III_A_4. Jak widać, w każdym z 500 pomiarów wykryto spoofing i poprawnie określono zbiór fałszywych sygnałów. Z kolei z Tab. 6.6 można odczytać parametry jakościowe eliminacji spoofingu. Średnia wartość sygnałów $\frac{C}{N_0}$ spoofera spadła, wskutek filtracji przestrzennej, o ponad 25 dB, z poziomu ponad 57 dBHz do poziomu ok. 32 dBHz. Natomiast średnia wartość $\frac{C}{N_0}$ sygnałów prawdziwych wzrosła z poziomu 32,7 dBHz o ponad 11 dB. Przed eliminacją spoofingu nie był odbierany żaden sygnał prawdziwy. Procedury antyspoofingowe umożliwiły odbiór prawdziwych sygnałów, przy czym najczęściej możliwy był odbiór trzech z nich (42,2% przypadków).

Pomiary w analogicznych warunkach przeprowadzono również dla scenariuszy, w których nadawane było od 5 do 8 sygnałów fałszywych. Wartości $\frac{C}{N_0}$ sygnałów odbieranych w trakcie

tych pomiarów, przed i po eliminacji spoofingu, przedstawiono na Rys. od 6.19 do 6.22.

W scenariuszu III_A_5 nadawano pięć sygnałów o numerach ciągów C/A: 9, 13, 17, 21 i 24, odbieranych ze średnim stosunkiem $\frac{C}{N_0}$ wynoszącym 56,8 dBHz. Sygnały o tak dużej mocy praktycznie uniemożliwiały wykrycie sygnałów prawdziwych. Jedynie w 9 na 500 akwizycji, blisko końca serii pomiarowej, wykryto pojedynczy prawdziwy sygnał. Najpierw był to sygnał o numerze 28, a później o numerze 1.

Po eliminacji spoofingu, średnia wartość $\frac{C}{N_0}$ sygnałów fałszywych spadła do wartości 31,8 dBHz, co jest równoznaczne z całkowitym wytłumieniem tych sygnałów. Eliminacja spoofingu umożliwiła odbiór sygnałów prawdziwych, przy czym najczęściej (w 38,8% przypadków) po filtracji przestrzennej wykrywano cztery takie sygnały. Na skutek eliminacji spoofingu średnia wartość $\frac{C}{N_0}$ sygnałów prawdziwych wzrosła o ponad 10 dB względem poziomu 33,4 dBHz. Wartości parametrów jakościowych detekcji i eliminacji spoofingu w scenariuszu III_A_5 są zawarte w Tab. 6.7 i 6.8. Podobnie jak poprzednio, w każdym z 500 pomiarów spoofing został wykryty i poprawnie określono numery fałszywych sygnałów.



Rysunek 6.19: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz III_A_5)

Tabela 6.7: Parametry jakościowe detekcji spoofingu w scenariuszu III_A_5

	N_{wyst}	Udział
N_{det}	500	100,0%
$N_{det\ OK}$	500	100,0%
$N_{det\ \subset S_{spoof}}$	0	0,0%
$N_{det\ \notin S_{spoof}}$	0	0,0%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	—	—
7	—	—
8	—	—

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

Tabela 6.8: Parametry jakościowe eliminacji spoofingu w scenariuszu III_A_5

$\overline{\frac{C}{N_0}}_{\in S_{spoof}}$	56,8 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}}$	33,4 dBHz
$\overline{\frac{C}{N_0}}_{\in S_{spoof}\ filtr}$	31,8 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}\ filtr}$	43,9 dBHz

$P_{\notin S_{spoof}}$

N_{sygn}	N_{wyst}	Udział
0	491	98,2%
1	9	1,8%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

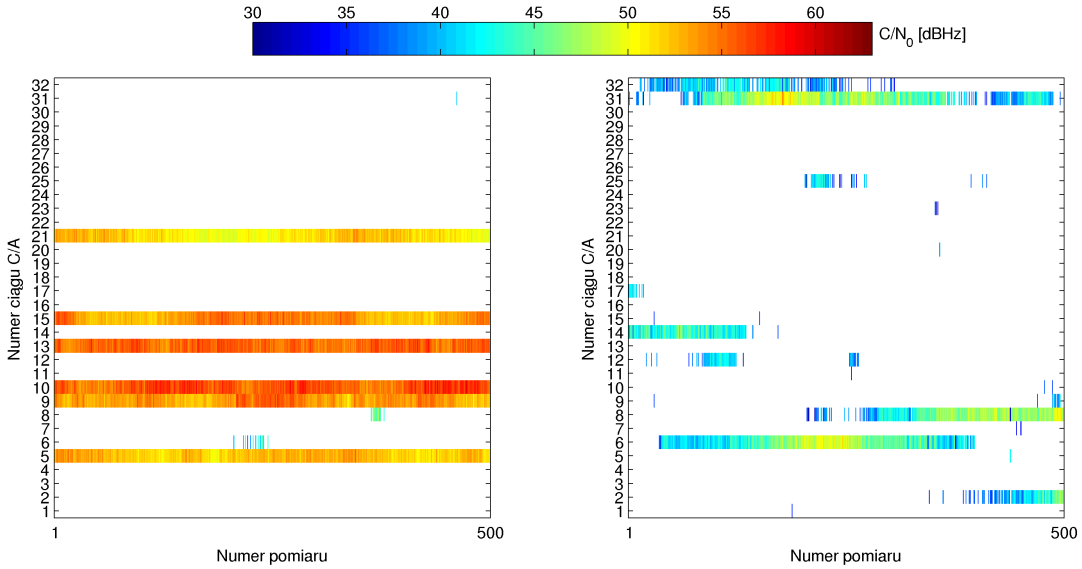
$P_{\notin S_{spoof}\ filtr}$

N_{sygn}	N_{wyst}	Udział
0	0	0,0%
1	0	0,0%
2	17	3,4%
3	125	25,0%
4	194	38,8%
5	138	27,6%
6	26	5,2%

W scenariuszu III_A_6 transmitowano sygnały fałszywe o numerach: 5, 9, 10, 13, 15 i 21, których średnia wartość $\frac{C}{N_0}$ przed eliminacją spoofingu wynosiła 53,7 dBHz. Podobnie jak w poprzednim scenariuszu, odnotowano sytuacje wykrycia pojedynczego sygnału prawdziwego obok sygnałów fałszywych. Takich przypadków, dotyczących sygnałów o numerach 6 i 8, było 26, co stanowi 5,2% wszystkich pomiarów w serii. W tym scenariuszu żaden z numerów odbieranych sygnałów prawdziwych nie pokrywał się z numerami sygnałów spoofera.

Parametry efektywności metod antyspoofingowych w tym scenariuszu przedstawiono w Tab. 6.9 i 6.10. Eliminacja spoofingu poprawiła możliwości odbioru sygnałów prawdziwych. W ponad połowie pomiarów wykrywano trzy sygnały z satelitów GPS. Stosunek $\frac{C}{N_0}$ sygnałów spoofera po

filtracji przestrzennej jest taki sam jak w poprzednim scenariuszu. Odnośnie sygnałów prawdziwych, ich średnie $\frac{C}{N_0}$ przed filtracją wynosiło 37,5 dBHz, a po filtracji wzrosło o 6 dB. Detekcja spoofingu, tak jak poprzednio, była bezbłędna.



Rysunek 6.20: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz III_A_6)

Tabela 6.9: Parametry jakościowe detekcji spoofingu w scenariuszu III_A_6

	N_{wyst}	Udział
N_{det}	500	100,0%
$N_{det\ OK}$	500	100,0%
$N_{det\ \subset S_{spoof}}$	0	0,0%
$N_{det\ \notin S_{spoof}}$	0	0,0%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%
7	—	—
8	—	—

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

Tabela 6.10: Parametry jakościowe eliminacji spoofingu w scenariuszu III_A_6

$\overline{\frac{C}{N_0} \in S_{spoof}}$	53,7 dBHz
$\overline{\frac{C}{N_0} \notin S_{spoof}}$	37,5 dBHz
$\overline{\frac{C}{N_0} \in S_{spoof\ \ filtr}}$	31,8 dBHz
$\overline{\frac{C}{N_0} \notin S_{spoof\ \ filtr}}$	43,5 dBHz

$P_{\notin S_{spoof}}$

N_{sygn}	N_{wyst}	Udział
0	474	94,8%
1	26	5,2%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

$P_{\notin S_{spoof\ \ filtr}}$

N_{sygn}	N_{wyst}	Udział
0	0	0,0%
1	14	2,8%
2	98	19,6%
3	259	51,8%
4	81	16,2%
5	47	9,4%
6	1	0,2%

Scenariusz III_A_7 dotyczy odbioru siedmiu sygnałów spoofera o numerach: 3, 5, 13, 15, 21, 24, 28. Średnia wartość $\frac{C}{N_0}$ tych sygnałów przed filtracją przestrzenną wynosi 56,2 dBHz. W tej serii pomiarowej, przed eliminacją spoofingu, nie odebrano żadnego prawdziwego sygnału GPS. Począwszy od 50. pomiaru, dwa sygnały o numerze 5 były odbierane równocześnie ze spoofera i satelity GPS. Taka sytuacja trwała przez ok. 70% długości serii pomiarowej.

Efektywność wykrywania i eliminacji spoofingu opisują wartości parametrów w Tab. 6.11 i 6.12. Filtracja przestrzenna spowodowała spadek $\frac{C}{N_0}$ sygnałów spoofera do wartości 31,7 dBHz oraz wzrost wartości $\frac{C}{N_0}$ sygnałów prawdziwych z wartości 32 dBHz o 12 dB. Po eliminacji spoofingu najczęściej był możliwy odbiór trzech lub czterech sygnałów prawdziwych (odpowiednio 32,4% i 37,6% przypadków).

Tabela 6.11: Parametry jakościowe detekcji spoofingu w scenariuszu III_A_7

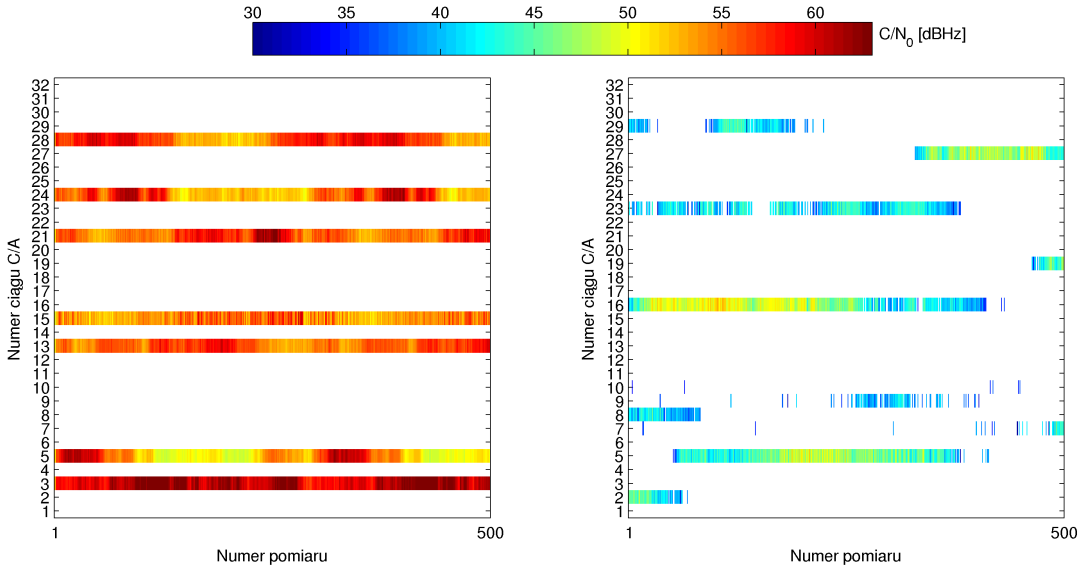
	N_{wyst}	Udział
N_{det}	500	100,0%
$N_{det\ OK}$	500	100,0%
$N_{det\ \subset S_{spoof}}$	0	0,0%
$N_{det\ \notin S_{spoof}}$	0	0,0%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%
7	0	0,0%
8	—	—

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%



Rysunek 6.21: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz III_A_7)

Tabela 6.12: Parametry jakościowe eliminacji spoofingu w scenariuszu III_A_7

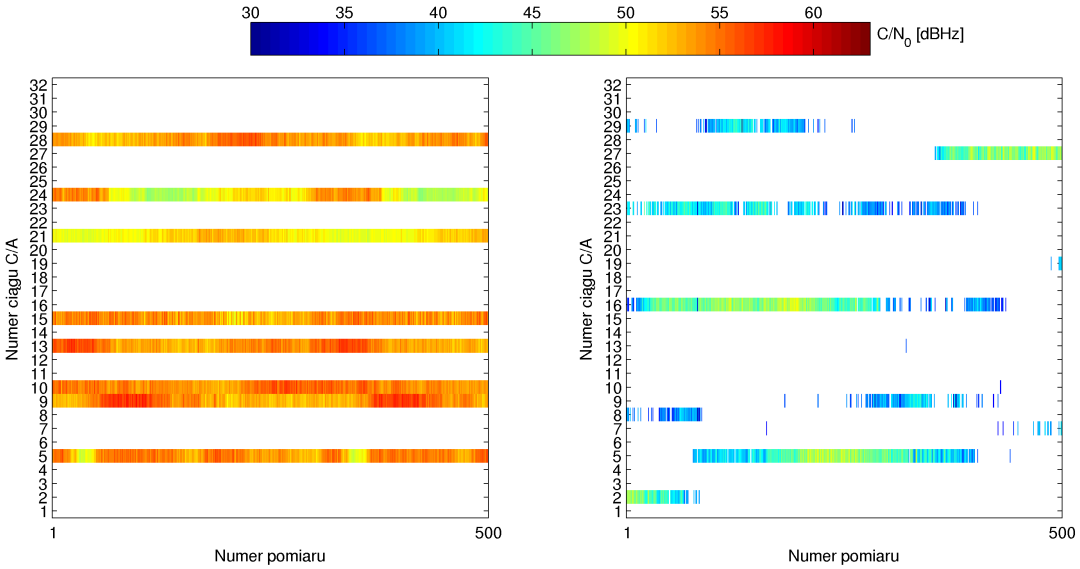
$\overline{\frac{C}{N_0}}_{\in S_{spoof}}$	56,2 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}}$	32,0 dBHz
$\overline{\frac{C}{N_0}}_{\in S_{spoof\ \ filtr}}$	31,7 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof\ \ filtr}}$	44,0 dBHz

$P_{\notin S_{spoof}}$			$P_{\notin S_{spoof\ \ filtr}}$		
N_{sygn}	N_{wyst}	Udział	N_{sygn}	N_{wyst}	Udział
0	500	100,0%	0	0	0,0%
1	0	0,0%	1	40	8,0%
2	0	0,0%	2	68	13,6%
3	0	0,0%	3	162	32,4%
4	0	0,0%	4	188	37,6%
5	0	0,0%	5	41	8,2%
6	0	0,0%	6	1	0,2%

W serii pomiarowej wg scenariusza III_A_8 nadawano 8 sygnałów spoofera o numerach ciągów C/A: 5, 9, 10, 13, 15, 21, 24 i 28. Średnia wartość stosunku $\frac{C}{N_0}$ tych sygnałów przed filtracją przestrzenną była równa 53,1 dBHz. Podobnie jak w pomiarach przeprowadzonych dla scenariuszy z czterema i siedmioma sygnałami fałszywymi, w akwizycjach wykonanych przed eliminacją spoofingu nie wykryto żadnych sygnałów prawdziwych. Dwa, spośród sygnałów odbieranych z satelitów GPS w trakcie serii pomiarowej, miały taki sam numer ciągu C/A jak

sygnały spoofera. Były to sygnały 5 i 9.

Parametry jakościowe procedur antyspoofinigowych w tej serii pomiarowej zostały zaprezentowane w Tab. 6.13 i 6.14. Tak jak we wszystkich poprzednich seriach, w każdym pomiarze dokonano prawidłowej detekcji spoofingu. Po eliminacji spoofingu najczęściej odbierano trzy (36,6% przypadków) lub cztery (30,6% przypadków) sygnały z satelitów GPS. Wartość $\frac{C}{N_0}$ sygnałów fałszywych spadła do poziomu 31,8 dBHz, a prawdziwych wzrosła z 36 dBHz do 42,9 dBHz.



Rysunek 6.22: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz III_A_8)

Wyniki wszystkich pomiarów przeprowadzonych w konfiguracji III wskazują na dużą skuteczność proponowanych rozwiązań antyspoofingowych. W szczególności detekcja spoofingu i określanie zbioru sygnałów fałszywych zostały wykonane prawidłowo w każdym przypadku. Po eliminacji spoofingu najczęściej był możliwy odbiór trzech lub czterech sygnałów z satelitów GPS, co jest zgodne z wynikami pomiarów widoczności satelitów w punkcie pomiarowym w przypadku braku spoofingu. We wszystkich scenariuszach średnia wartość $\frac{C}{N_0}$ sygnałów spoofera po filtracji przestrzennej mieściła się w zakresie 31,8±0,1 dBHz. Ten wynik był niezależny od średniej wartości $\frac{C}{N_0}$ tych sygnałów przed filtracją.

Tabela 6.13: Parametry jakościowe detekcji spoofingu w scenariuszu III_A_8

	N_{wyst}	Udział
N_{det}	500	100,0%
$N_{det\ OK}$	500	100,0%
$N_{det\ \subset S_{spoof}}$	0	0,0%
$N_{det\ \notin S_{spoof}}$	0	0,0%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%
7	0	0,0%
8	0	0,0%

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

Tabela 6.14: Parametry jakościowe eliminacji spoofingu w scenariuszu III_A_8

$\overline{\frac{C}{N_0}}_{\in S_{spoof}}$	53,1 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}}$	36,0 dBHz
$\overline{\frac{C}{N_0}}_{\in S_{spoof}\ filtr}$	31,8 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}\ filtr}$	42,9 dBHz

$P_{\notin S_{spoof}}$

N_{sygn}	N_{wyst}	Udział
0	500	100,0%
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

$P_{\notin S_{spoof}\ filtr}$

N_{sygn}	N_{wyst}	Udział
0	0	0,0%
1	55	11,0%
2	99	19,8%
3	183	36,6%
4	153	30,6%
5	9	1,8%
6	1	0,2%

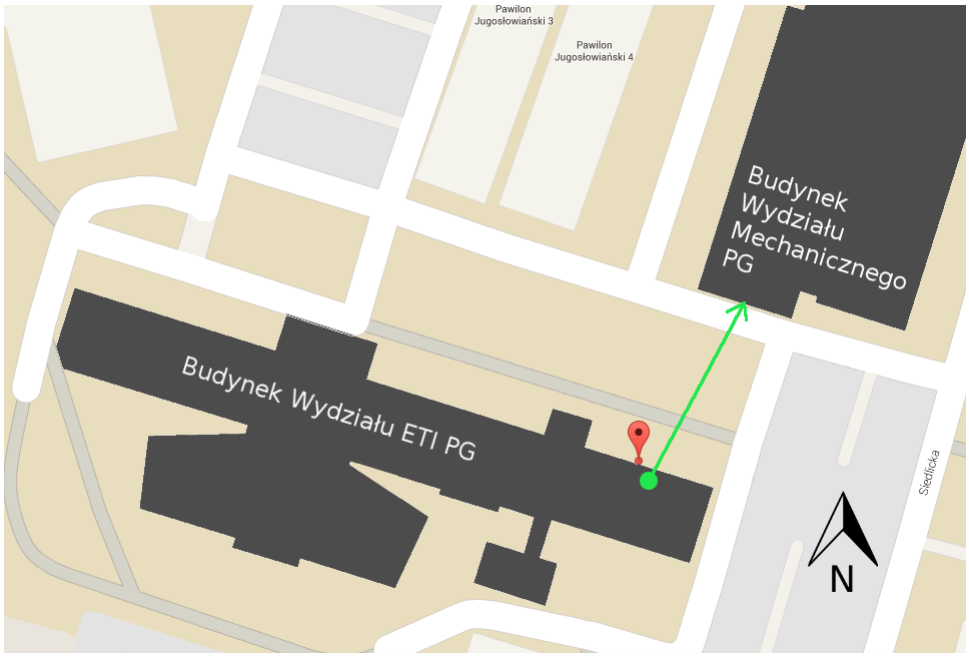
6.5 Analiza wyników IV etapu badań

Wyniki uzyskane w III konfiguracji pomiarowej pozwalają wnioskować, że, w przypadku odbioru sygnałów spoofera o mocy znacznie przekraczającej moc sygnałów prawdziwych, proponowane metody antyspoofingowe charakteryzują się dużą skutecznością. Jednakże, ostateczna weryfikacja ich efektywności wymaga realizacji pomiarów w IV konfiguracji stanowiska pomiarowego, w której sygnały spoofera są przesyłane w rzeczywistym kanale radiowym.

6.5.1 Efektywność procedur antyspoofingowych - transmisja radiowa

Pomiary, uwzględniające bezprzewodową transmisję sygnałów spoofera, przeprowadzono dla scenariuszy analogicznych do tych przyjętych w konfiguracji III, tj. przy nadawaniu od 4 do 8 sygnałów fałszywych.

Zarówno system antyspoofingowy, jak i spoofer, znajdowały się w jednym pomieszczeniu. Odbiorczy szyk antenowy ustawiono w tym samym miejscu, co w poprzednich seriach pomiarowych, natomiast antena kierunkowa transmitująca sygnały fałszywe została ulokowana wewnątrz budynku. Pomiędzy antenami odbiorczymi a nadawczą znajdował się zbrojony filar konstrukcji budynku WETI, wobec czego był to przypadek transmisji typu NLoS. Wiązka główna charakterystyki promieniowania anteny spoofera w płaszczyźnie poziomej została skierowana na północny-północny wschód (NNE). Takie ustawienie anteny było podyktowane tym, aby najsilniejsza składowa sygnału odbieranego stanowiła sygnał odbity od elewacji południowej budynku Wydziału Mechanicznego PG. Na Rys. 6.23 zgrubne położenie anteny nadawczej oznaczono zieloną kropką, a kierunek jej wiązki głównej - zieloną strzałką [30].



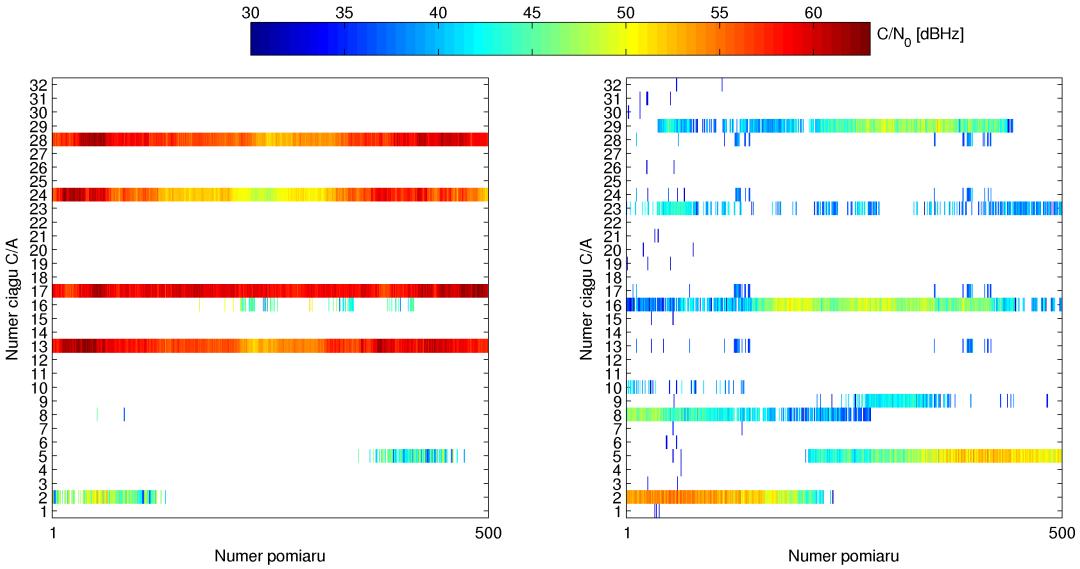
Rysunek 6.23: Położenie i orientacja pozioma anteny nadawczej spoofera

Istnieje ryzyko, że bezprzewodowa transmisja sygnałów spoofera mogłaby spowodować zakłócenia pracy pobliskich odbiorników GPS. W związku z tym, było konieczne zmniejszenie mocy tych sygnałów na wyjściu generatora, w stosunku do wartości zastosowanych w konfiguracji III. Moc każdego z sygnałów spoofera została zredukowana do wartości odpowiadającej

poziomowi mocy silnego sygnału prawdziwego, docierającego z satelity GPS.

Wartości $\frac{C}{N_0}$, zmierzone przed i po eliminacji spoofingu w scenariuszach dla konfiguracji IV, przedstawiono, w formie wykresów pseudokolorowych, na Rys. od 6.24 do 6.28. Można na nich dostrzec zwiększenie liczby przypadków akwizycji sygnałów prawdziwych przed eliminacją spoofingu, w stosunku do liczby analogicznych obserwacji dla konfiguracji III. Jest to spowodowane zmniejszeniem mocy nadawanych sygnałów fałszywych.

W scenariuszu IV_A_4 spoofer nadawał sygnały o numerach ciągów C/A: 13, 17, 24 i 28. Żaden z sygnałów prawdziwych, odbieranych w trakcie serii pomiarowej, nie miał numeru ciągu C/A z tego zbioru. Średnia wartość $\frac{C}{N_0}$ sygnałów fałszywych przed filtracją przestrzenną wynosiła 57 dBHz. Od początku serii pomiarowej był odbierany silny sygnał prawdziwy o numerze 2, który był wykrywany także przed eliminacją spoofingu. W drugiej połowie serii pomiarowej z podobną mocą był odbierany sygnał z numerem 5.



Rysunek 6.24: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz IV_A_4)

Parametry jakościowe dla tego scenariusza przedstawiono w Tab. 6.15 i 6.16. Tak jak w pomiarach dla konfiguracji III, także w tym przypadku dokonano bezbłędnej detekcji spoofingu

i określenia numerów fałszywych sygnałów. W niemal połowie pomiarów (46,8%) w pierwszej akwizycji wykryto co najmniej jeden sygnał prawdziwy. W drugiej akwizycji, dokonywanej po filtracji przestrzennej, najczęściej (40,6% przypadków) wykrywano cztery sygnały z satelitów GPS. Filtracja przestrzenna spowodowała spadek średniego $\frac{C}{N_0}$ sygnałów spoofera do poziomu 32,3 dBHz i wzrost średniego $\frac{C}{N_0}$ sygnałów prawdziwych z 39,2 dBHz do 44,5 dBHz.

Tabela 6.15: Parametry jakościowe detekcji spoofingu w scenariuszu IV_A_4

	N_{wyst}	Udział
N_{det}	500	100,0%
$N_{det\ OK}$	500	100,0%
$N_{det\ \subset S_{spoof}}$	0	0,0%
$N_{det\ \notin S_{spoof}}$	0	0,0%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	—	—
6	—	—
7	—	—
8	—	—

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

Tabela 6.16: Parametry jakościowe eliminacji spoofingu w scenariuszu IV_A_4

$\overline{\frac{C}{N_0}}_{\in S_{spoof}}$	57,0 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}}$	39,2 dBHz
$\overline{\frac{C}{N_0}}_{\in S_{spoof}\ filtr}$	32,3 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}\ filtr}$	44,5 dBHz

$P_{\notin S_{spoof}}$

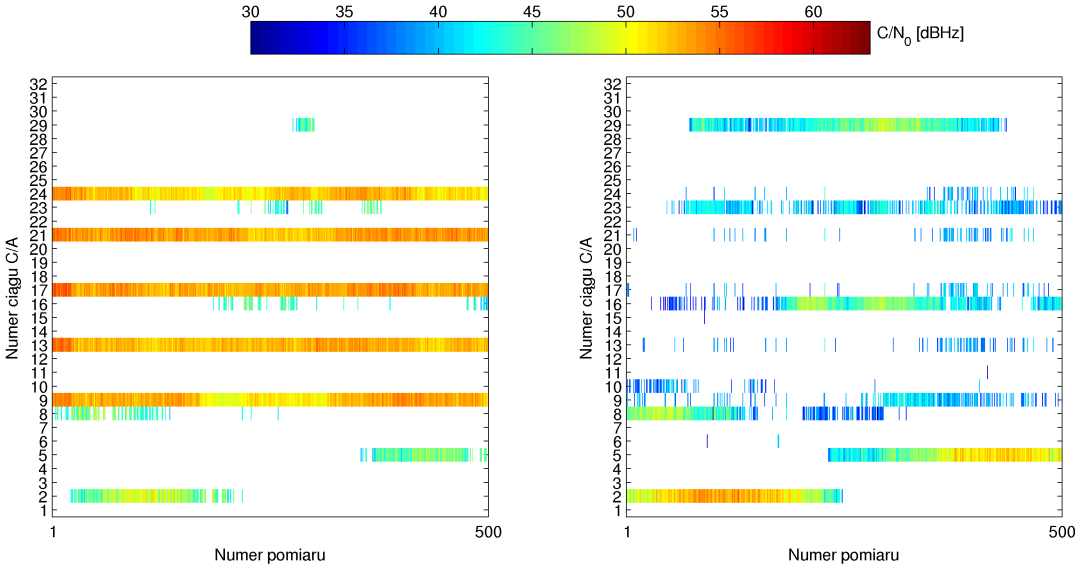
N_{sygn}	N_{wyst}	Udział
0	266	53,2%
1	219	43,8%
2	15	3,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

$P_{\notin S_{spoof}\ filtr}$

N_{sygn}	N_{wyst}	Udział
0	0	0,0%
1	2	0,4%
2	41	8,2%
3	114	22,8%
4	203	40,6%
5	103	20,6%
6	29	5,8%

W serii pomiarowej dla scenariusza IV_A_5 sygnały nadawane przez spoofer miały numery: 9, 13, 17, 21 i 24. Średnia wartość $\frac{C}{N_0}$ tych sygnałów, zmierzona przed filtracją przestrzenną, wynosi 52,8 dBHz. Do punktu pomiarowego docierał również prawdziwy sygnał z numerem 9. Można zauważyć podobieństwo pomiędzy wykresami $\frac{C}{N_0}$ po eliminacji spoofingu na Rys. 6.24

i 6.25. Wynika ono z faktu, że pomiary dla scenariuszy IV_A_4 i IV_A_5 rozpoczęto o podobnej godzinie w dwóch bezpośrednio następujących po sobie dniach.



Rysunek 6.25: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz IV_A_5)

Parametry detekcji i eliminacji spoofingu opisano w Tab. 6.17 i 6.18. W przypadku tej serii pomiarowej spoofing był wykrywany za każdym razem, jednakże odnotowano przypadki nieprawidłowego określenia zbioru numerów sygnałów fałszywych. W 41 pomiarach, co stanowi 8,2% spośród całej serii, uznano co najmniej jeden sygnał prawdziwy za kolejny sygnał pochodzący ze spoofera. Oznacza to, że opóźnienia fazowe tego sygnału i sygnałów spoofera były na tyle podobne, że ich różnice były mniejsze niż próg detekcji, ustalony dla liczby sygnałów fałszywych większej od pięciu. W 38 pomiarach błędnie uznano jeden sygnał prawdziwy za fałszywy, a w trzech innych pomiarach taką decyzję podjęto odnośnie trzech sygnałów prawdziwych.

Przed filtracją przestrzenną najczęściej (58,4% przypadków) w pierwszej akwizycji wykrywano jeden sygnał prawdziwy. Po filtracji przestrzennej najczęściej były to cztery sygnały (32,8% przypadków). Średnia wartość $\frac{C}{N_0}$ sygnałów spoofera po filtracji przestrzennej to 33,1 dBHz. Wartość $\frac{C}{N_0}$ sygnałów prawdziwych była stosunkowo wysoka już przed eliminacją spoofingu i wynosiła 41,1 dBHz. Po eliminacji odnotowano wzrost tej wartości o 3,1 dB.

Tabela 6.17: Parametry jakościowe detekcji spoofingu w scenariuszu IV_A_5

	N_{wyst}	Udział
N_{det}	500	100,0%
$N_{det\ OK}$	459	91,8%
$N_{det\ \subset S_{spoof}}$	0	0,0%
$N_{det\ \notin S_{spoof}}$	41	8,2%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	—	—
7	—	—
8	—	—

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	38	7,6%
2	0	0,0%
3	3	0,6%
4	0	0,0%
5	0	0,0%
6	0	0,0%

Tabela 6.18: Parametry jakościowe eliminacji spoofingu w scenariuszu IV_A_5

$\overline{\frac{C}{N_0} \in S_{spoof}}$	52,8 dBHz
$\overline{\frac{C}{N_0} \notin S_{spoof}}$	41,1 dBHz
$\overline{\frac{C}{N_0} \in S_{spoof\ \ filtr}}$	33,1 dBHz
$\overline{\frac{C}{N_0} \notin S_{spoof\ \ filtr}}$	44,2 dBHz

$P_{\notin S_{spoof}}$

N_{sygn}	N_{wyst}	Udział
0	110	22,0%
1	292	58,4%
2	95	19,0%
3	3	0,6%
4	0	0,0%
5	0	0,0%
6	0	0,0%

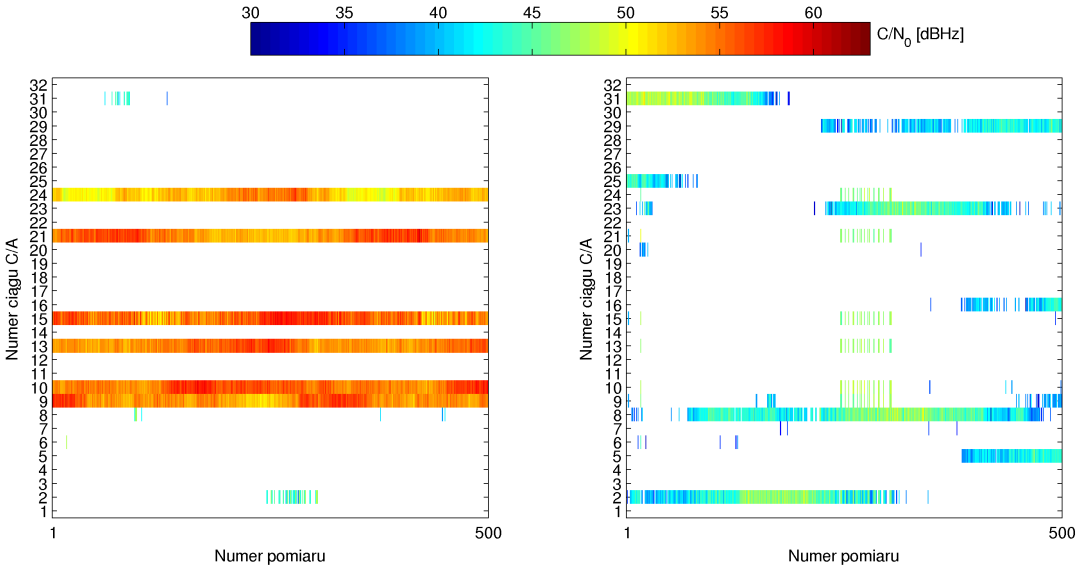
$P_{\notin S_{spoof\ \ filtr}}$

N_{sygn}	N_{wyst}	Udział
0	0	0,0%
1	6	1,2%
2	82	16,4%
3	124	24,8%
4	164	32,8%
5	106	21,2%
6	18	3,6%

Scenariusz IV_A_6 obejmuje transmisję sygnałów o numerach: 9, 10, 13, 15, 21 i 24. Żaden z sygnałów prawdziwych o tych numerach nie był odbierany w czasie serii pomiarowej. Średnia wartość $\frac{C}{N_0}$ sygnałów prawdziwych przed filtracją to 54,4 dBHz.

Parametry jakościowe wykrywania i eliminacji spoofingu zapisano w Tab. 6.19 i 6.20. Także w przypadku tego scenariusza odnotowano przypadki uznania jednego prawdziwego sygnału GPS za fałszywy, jednakże ich odsetek był mniejszy niż w scenariuszu IV_A_5 i wynosił 4,4%.

W 10,2% przypadków przed eliminacją spoofingu wykrywano pojedynczy prawdziwy sygnał GPS. Po eliminacji najczęściej były to trzy sygnały (47,6% pomiarów). Wartość $\frac{C}{N_0}$ sygnałów fałszywych spadła po filtracji do poziomu 32,3 dBHz, a sygnałów prawdziwych wzrosła z 37,9 dBHz do 43,2 dBHz.



Rysunek 6.26: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz IV_A_6)

Tabela 6.19: Parametry jakościowe detekcji spoofingu w scenariuszu IV_A_6

	N_{wyst}	Udział
N_{det}	500	100,0%
$N_{det\ OK}$	478	95,6%
$N_{det\ \subset S_{spoof}}$	0	0,0%
$N_{det\ \notin S_{spoof}}$	22	4,4%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%
7	—	—
8	—	—

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	22	4,4%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

Tabela 6.20: Parametry jakościowe eliminacji spoofingu w scenariuszu IV_A_6

$\overline{\frac{C}{N_0} \in S_{spoof}}$	54,4 dBHz
$\overline{\frac{C}{N_0} \notin S_{spoof}}$	37,9 dBHz
$\overline{\frac{C}{N_0} \in S_{spoof\ \ filtr}}$	32,3 dBHz
$\overline{\frac{C}{N_0} \notin S_{spoof\ \ filtr}}$	43,2 dBHz

$P_{\notin S_{spoof}}$

N_{sygn}	N_{wyst}	Udział
0	449	89,8%
1	51	10,2%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

$P_{\notin S_{spoof}\ \ filtr}$

N_{sygn}	N_{wyst}	Udział
0	0	0,0%
1	10	2,0%
2	73	14,6%
3	238	47,6%
4	127	25,4%
5	50	10,0%
6	2	0,4%

W przypadku scenariusza IV_A_7 transmitowano sygnały o numerach ciągów: 5, 9, 13, 17, 21, 24 i 28. Ich średnia wartość $\frac{C}{N_0}$ przed filtracją przestrzenną to 52,2 dBHz. Przez ok. 100 pierwszych pomiarów w serii był odbierany również sygnał prawdziwy o numerze 17. Ponadto, do szyku antenowego docierały silne sygnały z satelitów o numerach 6 i 31. Wartość $\frac{C}{N_0}$ tych sygnałów po filtracji przestrzennej w niektórych przypadkach przekraczała 52 dBHz.

Wartości parametrów jakościowych procedur antyspoofingowych przedstawiono w Tab. 6.21 i 6.22. W przypadku tej serii pomiarowej można zauważyć wyraźne pogorszenie poprawności określania zbioru numerów sygnałów fałszywych. Zbiór ten został wyznaczony prawidłowo jedynie w 48% przypadków. W pozostałych 52% błędnie uznano jeden z sygnałów prawdziwych za kolejny sygnał spoofera. Wiąże się to z tym, że wartości progowe różnic opóźnień fazowych, poniżej których uznaje się sygnał GPS za fałszywy, są stosunkowo wysokie w przypadku odbioru ośmiu sygnałów fałszywych (vide Rys. 4.11 i Tab. 4.2). Zatem, przy równoczesnym wykryciu siedmiu sygnałów fałszywych i co najmniej jednego prawdziwego, jest wysoce prawdopodobne, że sygnał prawdziwy zostanie uznany za fałszywy.

Tabela 6.21: Parametry jakościowe detekcji spoofingu w scenariuszu IV_A_7

	N_{wyst}	Udział
N_{det}	500	100,0%
$N_{det\ OK}$	240	48,0%
$N_{det\ \subset S_{spoof}}$	0	0,0%
$N_{det\ \notin S_{spoof}}$	260	52,0%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

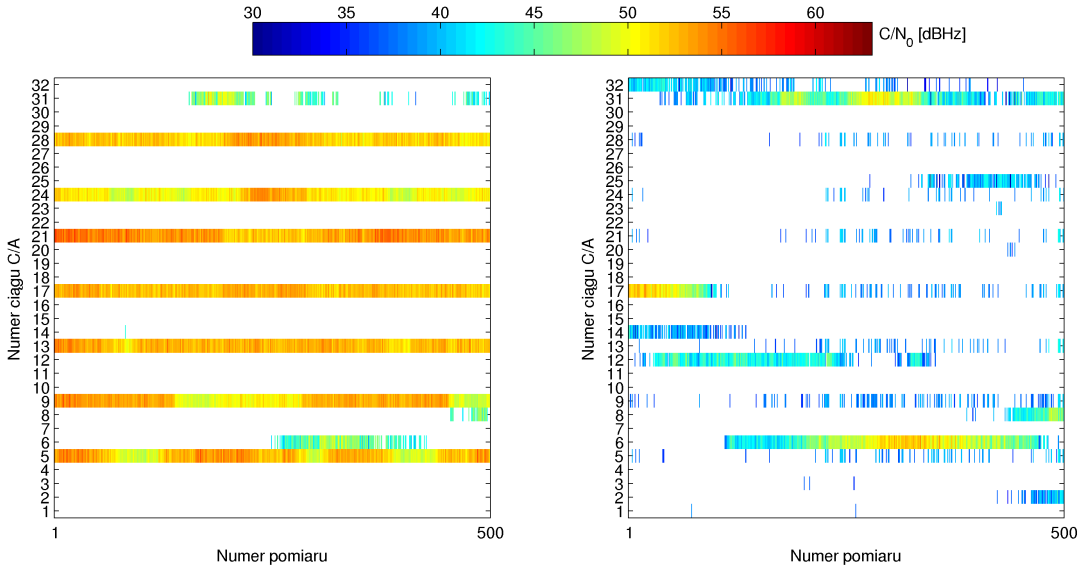
$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%
7	0	0,0%
8	—	—

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	260	52,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

Przed eliminacją spoofingu w tym scenariuszu najczęściej nie był wykrywany żaden sygnał prawdziwy (48% pomiarów) lub był wykrywany jeden z nich (41,8%). Po eliminacji najczęściej wykrywano trzy sygnały prawdziwe (50,6% pomiarów). Średnia wartość $\frac{C}{N_0}$ sygnałów spoofera została zredukowana do 34 dBHz, a dla sygnałów prawdziwych wzrosła z 40 dBHz do 43 dBHz.



Rysunek 6.27: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz IV_A_7)

Tabela 6.22: Parametry jakościowe eliminacji spoofingu w scenariuszu IV_A_7

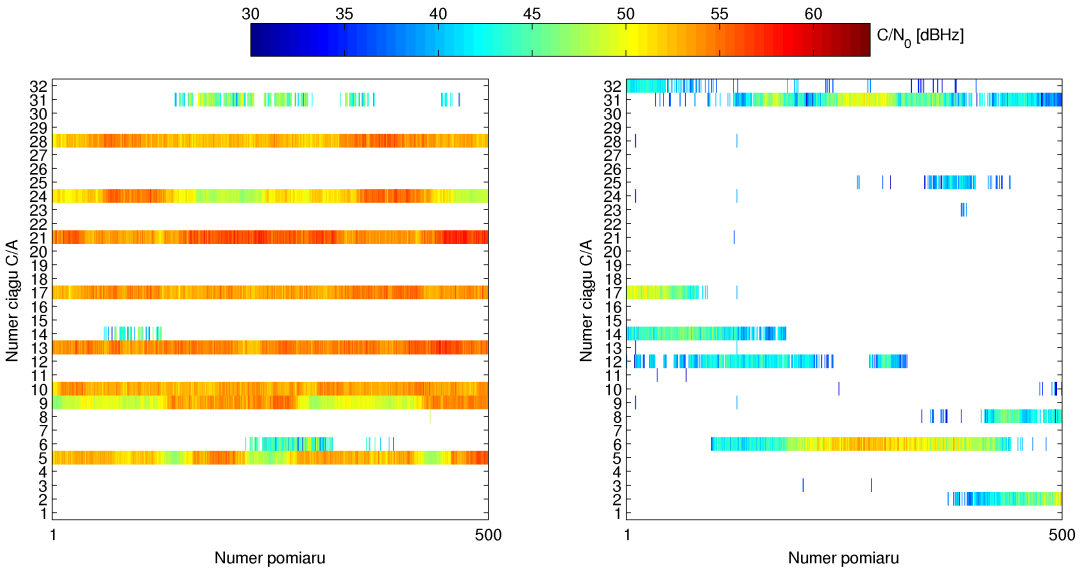
$\overline{\frac{C}{N_0}}_{\in S_{spoof}}$	52,2 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}}$	40,0 dBHz
$\overline{\frac{C}{N_0}}_{\in S_{spoof\ filtr}}$	34,0 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof\ filtr}}$	43,0 dBHz

$P_{\notin S_{spoof}}$			$P_{\notin S_{spoof\ filtr}}$		
N_{sygn}	N_{wyst}	Udział	N_{sygn}	N_{wyst}	Udział
0	240	48,0%	0	0	0,0%
1	209	41,8%	1	2	0,4%
2	51	10,2%	2	81	16,2%
3	0	0,0%	3	253	50,6%
4	0	0,0%	4	127	25,4%
5	0	0,0%	5	36	7,2%
6	0	0,0%	6	1	0,2%

W serii pomiarowej dla scenariusza IV_A_8 były przesyłane sygnały o numerach: 5, 9, 10, 13, 17, 21, 24 i 28. Numery i moce odbieranych sygnałów prawdziwych były podobne do tych obserwowanych w poprzednim scenariuszu, gdyż obie serie pomiarowe przeprowadzono w dwóch kolejnych dniach, w zbliżonych godzinach. Średnia wartość $\frac{C}{N_0}$ odbieranych sygnałów spoofera przed filtracją była równa 53 dBHz.

Parametry liczbowe detekcji i eliminacji spoofingu przedstawiono w Tab. 6.23 i 6.24. W przypadku tego scenariusza, w każdym pomiarze dokonano prawidłowego określenia zbioru fałszywych sygnałów. Było to możliwe dzięki przyjętemu odgórnemu ograniczeniu - do ośmiu - liczby sygnałów spoofera, które mogą być równocześnie odbierane. Można rozważyć sytuację, w której jest odbieranych osiem sygnałów spoofera i jeden lub więcej sygnałów prawdziwych. Nawet jeśli różnice opóźnień fazowych pomiędzy sygnałem prawdziwym i sygnałami spoofera są mniejsze niż próg detekcji, to sygnał prawdziwy nie zostanie uznany za fałszywy. Zostanie za nie uznane te osiem sygnałów, dla których różnice opóźnień fazowych są najmniejsze. Będą to więc w istocie sygnały nadawane przez spoofer, o ile sygnał prawdziwy nie nadchodzi z tego samego kierunku co one.

Przed eliminacją spoofingu w scenariuszu IV_A_8 w większości (53,8%) przypadków nie obierano żadnego sygnału prawdziwego. Po filtracji przestrzennej najczęściej odbierano trzy takie sygnały (47,2% przypadków). Wskutek eliminacji spoofingu średnia wartość $\frac{C}{N_0}$ sygnałów fałszywych zmalała do 31,8 dBHz, a średnia wartość $\frac{C}{N_0}$ sygnałów prawdziwych wzrosła z 39,1 dBHz do 44,2 dBHz.



Rysunek 6.28: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz IV_A_8)

Tabela 6.23: Parametry jakościowe detekcji spoofingu w scenariuszu IV_A_8

	N_{wyst}	Udział
N_{det}	500	100,0%
$N_{det\ OK}$	500	100,0%
$N_{det\ \subset S_{spoof}}$	0	0,0%
$N_{det\ \notin S_{spoof}}$	0	0,0%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%
7	0	0,0%
8	0	0,0%

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

Tabela 6.24: Parametry jakościowe eliminacji spoofingu w scenariuszu IV_A_8

$\overline{\frac{C}{N_0} \in S_{spoof}}$	53,0 dBHz
$\overline{\frac{C}{N_0} \notin S_{spoof}}$	39,1 dBHz
$\overline{\frac{C}{N_0} \in S_{spoof\ \ filtr}}$	31,8 dBHz
$\overline{\frac{C}{N_0} \notin S_{spoof\ \ filtr}}$	44,2 dBHz

$P_{\notin S_{spoof}}$

N_{sygn}	N_{wyst}	Udział
0	269	53,8%
1	187	37,4%
2	44	8,8%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

$P_{\notin S_{spoof\ \ filtr}}$

N_{sygn}	N_{wyst}	Udział
0	0	0,0%
1	1	0,2%
2	93	18,6%
3	236	47,2%
4	154	30,8%
5	16	3,2%
6	0	0,0%

Analiza wartości parametrów jakościowych dla scenariuszy w konfiguracji IV, wskazuje, że wystąpiło tu pogorszenie, względem wyników uzyskanych w konfiguracji III, poprawności określania liczby sygnałów fałszywych. Jest to spowodowane mniejszą mocą odbieranych sygnałów spoofera i, co za tym idzie, większą liczbą sygnałów prawdziwych wykrywanych przed eliminacją spoofingu. Progi detekcji spoofingu, których wartości określono w badaniach symulacyjnych, zostały wyznaczone dla przypadków spoofingu, gdzie w akwizycji są wykrywane jedynie sygnały fałszywe. Jeśli przed eliminacją spoofingu są odbierane równocześnie sygnały fałszywe i prawdziwe, co najmniej jeden z sygnałów z satelitów GPS może zostać uznany za sygnał pochodzący ze spoofera. Prawdopodobieństwo wystąpienia takiej błędnej klasyfikacji jest tym większe, im większa jest wartość progu detekcji spoofingu, ustalonego dla rzeczywistej liczby sygnałów fał-

szywych powiększonej o jeden.

Bezbłędne określenie zbiorów sygnałów fałszywych zaobserwowano w scenariuszach IV_A_4 i IV_A_8. W pierwszym z nich wynika to z faktu, że próg detekcji spoofingu przy pięciu sygnałach fałszywych jest jeszcze stosunkowo mały i różnice opóźnień fazowych pomiędzy sygnałem prawdziwym a czterema sygnałami spoofera są zwykle większe od tego progu.

W przypadku drugiego z wymienionych scenariuszy, numery wszystkich sygnałów spoofera zostały określone poprawnie, ponieważ stanowiły one osiem spośród sygnałów odbieranych, pomiędzy którymi różnice opóźnień fazowych były najmniejsze. Przyjęto, że może być odbieranych maksymalnie 8 sygnałów spoofera. Zatem sygnały o większych różnicach opóźnień fazowych nie zostaną uznane za fałszywe, nawet jeśli te różnice są mniejsze niż próg detekcji.

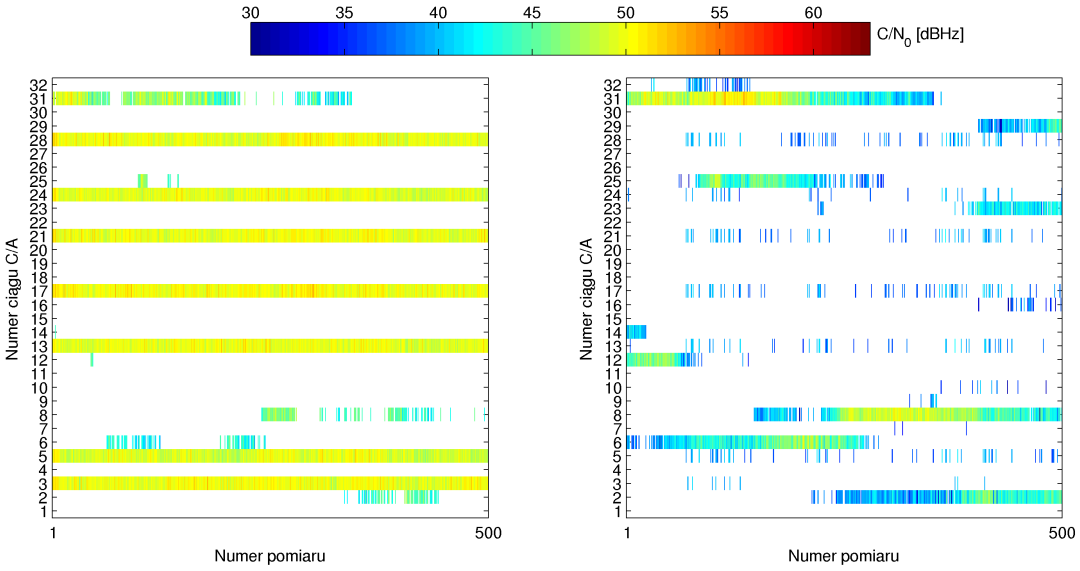
W seriach pomiarowych dotyczących scenariuszy IV_A_5, IV_A_6, i IV_A_7 odsetek liczby pomiarów z błędnym określeniem zbioru sygnałów fałszywych wyniósł odpowiednio: 8,2%, 4,4% i 52%. Gdyby serie pomiarowe były przeprowadzane w identycznych warunkach, liczba błędnych detekcji powinna wzrastać wraz z liczbą sygnałów fałszywych. Tymczasem przy sześciu fałszywych sygnałach jest ona mniejsza niż przy pięciu. Przyczyną tego jest mała liczba sygnałów prawdziwych wykrywanych przed eliminacją spoofingu w scenariuszu IV_A_6. W seriach dla scenariuszy IV_A_5 i IV_A_7 co najmniej jeden sygnał prawdziwy był wykrywany przed eliminacją w, odpowiednio, 78% i 52% pomiarów, podczas gdy dla scenariusza IV_A_6 jedynie w 10,2%.

Biorąc pod uwagę efektywność eliminacji spoofingu, można powiedzieć, że nie jest ona wyraźnie gorsza od tej obserwowanej w konfiguracji III. Średnia wartość $\frac{C}{N_0}$ sygnałów fałszywych po filtracji przestrzennej nie przekracza 34 dBHz, co oznacza, że zostały one stłumione do poziomu na granicy możliwości odbioru. Natomiast średni stosunek $\frac{C}{N_0}$ sygnałów prawdziwych po filtracji przestrzennej oscyluje około 43,5 dBHz, co jest wartością zbliżoną do obserwowanej w pomiarach w konfiguracji III.

6.5.2 Wpływ zmniejszenia progu detekcji na identyfikację sygnałów fałszywych

Rozwiązaniem, umożliwiającym ograniczenie częstości uznawania prawdziwych sygnałów GPS za sygnały spoofera, może być zmniejszenie progów detekcji spoofingu w przypadkach odbioru dużej liczby sygnałów GPS, np. powyżej sześciu. Obniżenie wartości progowych skutkuje mniejszym prawdopodobieństwem detekcji spoofingu w zakresie małych wartości $\frac{C}{N_0}$ (vide Rys. 4.12) Niemniej nie wpływa ono istotnie na prawdopodobieństwo detekcji przy wartościach $\frac{C}{N_0}$ powyżej 50 dBHz, a zwykle właśnie takie będą miały sygnały spoofera, docierające do odbiornika GPS.

Aby określić wpływ zmniejszenia progu detekcji spoofingu na poprawność identyfikacji numerów sygnałów fałszywych, przeprowadzono pomiary według scenariusza IV_B_7. Zasadnicza różnica pomiędzy tym scenariuszem, a scenariuszem IV_A_7 polega na tym, że jeśli podczas pierwszej akwizycji jest wykrytych siedem lub więcej sygnałów GPS, wartość progu detekcji jest dobierana tak, jakby było odbieranych jedynie sześć sygnałów fałszywych.



Rysunek 6.29: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz IV_B_7)

Wartości $\frac{C}{N_0}$ sygnałów przed i po filtracji przestrzennej przedstawiono na Rys. 6.29. Transmitowano sygnały o numerach: 3, 5, 13, 17, 21, 24 i 28. Średni stosunek $\frac{C}{N_0}$ tych sygnałów przed filtracją przestrzenną wynosił 49,7 dBHz. Jest to wartość o 2,5 dB mniejsza od tej ze scenariusza IV_A_7, co skutkuje większą liczbą prawdziwych sygnałów GPS wykrywanych przed eliminacją spoofingu, a tym samym zwiększa prawdopodobieństwo uznania sygnału prawdziwego za fałszywy.

Parametry jakościowe detekcji spoofingu przedstawiono w Tab. 6.25. Tym razem, poprawnej detekcji spoofingu i prawidłowego określenia numerów sygnałów fałszywych dokonano w 88,6% przypadków. Pomimo trudniejszych warunków, widać tu znaczącą poprawę w stosunku do scenariusza IV_A_7, gdzie było to jedynie 48% przypadków.

Tabela 6.25: Parametry jakościowe detekcji spoofingu w scenariuszu IV_B_7

	N_{wyst}	Udział
N_{det}	500	100,0%
$N_{det\ OK}$	443	88,6%
$N_{det\ \subset S_{spoof}}$	0	0,0%
$N_{det\ \notin S_{spoof}}$	57	11,4%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%
7	0	0,0%
8	—	—

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	57	11,4%
2	0	0,0%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

Tabela 6.26: Parametry jakościowe eliminacji spoofingu w scenariuszu IV_B_7

$\overline{\frac{C}{N_0}}_{\in S_{spoof}}$	49,7 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}}$	41,2 dBHz
$\overline{\frac{C}{N_0}}_{\in S_{spoof}\ filtr}$	32,8 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}\ filtr}$	43,8 dBHz

$P_{\notin S_{spoof}}$

N_{sygn}	N_{wyst}	Udział
0	103	20,6%
1	313	62,6%
2	75	15,0%
3	9	1,8%
4	0	0,0%
5	0	0,0%
6	0	0,0%

$P_{\notin S_{spoof}\ filtr}$

N_{sygn}	N_{wyst}	Udział
0	0	0,0%
1	4	0,8%
2	44	8,8%
3	197	39,4%
4	217	43,4%
5	37	7,4%
6	1	0,2%

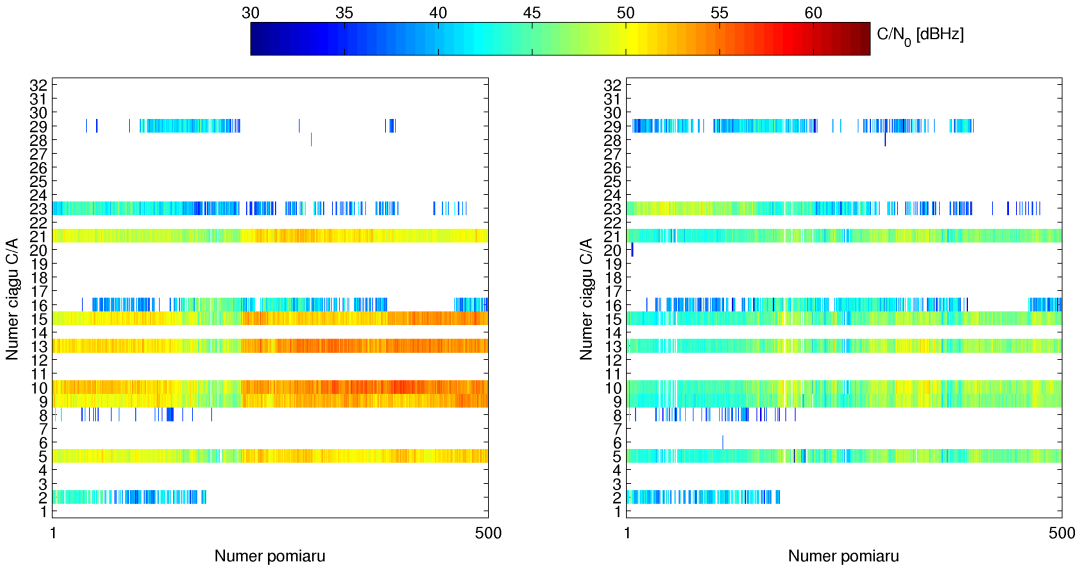
Poprawa jakości detekcji spoofingu zarazem wpłynęła korzystnie na jakość jego eliminacji. Wartości parametrów eliminacji zawarto w Tab. 6.26. W porównaniu ze scenariuszem IV_A_7, średnia wartość $\frac{C}{N_0}$ sygnałów fałszywych po filtracji przestrzennej jest mniejsza o 1,2 dB, a sygnałów prawdziwych - większa o 0,8 dB. Z trzech do czterech zwiększyła się również najczęstsza liczba sygnałów prawdziwych odbieranych po filtracji przestrzennej.

6.5.3 Wpływ propagacji wielodrogowej na efektywność antyspoofingu

Wszystkie opisane powyżej pomiary, wykonane w konfiguracji IV, przeprowadzono przy takim wzajemnym ustawieniu anteny nadawczej i odbiorczego szyku antenowego, gdzie w odbieranym sygnale spoofera była obecna składowa dominująca, związana z jednym kierunkiem nadejścia sygnału. W przypadku środowisk charakteryzujących się silną propagacją wielodrogową, dysproporcja mocy bezpośredniego i odbitych sygnałów spoofera, docierających z różnych kierunków, może być mniejsza.

Efektywność proponowanych procedur antyspoofingowych, w warunkach propagacji wielodrogowej, została zbadana poprzez pomiary przeprowadzone według scenariusza IV_C_6. W tym scenariuszu nadawano 6 sygnałów fałszywych poprzez antenę, która została obrócona o kilkanaście stopni w lewo, w stosunku do orientacji przyjętej w dotychczasowych scenariuszach dla konfiguracji IV. Takie ustawienie spowodowało zmniejszenie różnic pomiędzy mocami replik sygnałów odbieranych z różnych kierunków.

Zmierzone wartości $\frac{C}{N_0}$ zostały przedstawione w postaci wykresu na Rys. 6.30. Spoofer transmitował sygnały o numerach: 5, 9, 10, 13, 15 i 21. Średnia wartość $\frac{C}{N_0}$ tych sygnałów przed eliminacją spoofingu wynosiła 51,2 dBHz. Jak można zauważyć, po filtracji przestrzennej wartości $\frac{C}{N_0}$ tych sygnałów zmalały, lecz nie na tyle, żeby uznać to stłumienie za ich całkowitą eliminację. Jest to spowodowane tym, że przyjęty wariant metody kształtowania zer charakterystyki ustala zero tylko na jednym kierunku nadejścia sygnału, a składowe sygnału docierające innymi drogami są tłumione w znacznie mniejszym stopniu.



Rysunek 6.30: Wartości $\frac{C}{N_0}$ sygnałów przed i po eliminacji spoofingu (scenariusz IV_C_6)

Tabela 6.27: Parametry jakościowe detekcji spoofingu w scenariuszu IV_C_6

	N_{wyst}	Udział
N_{det}	498	99,6%
$N_{det\ OK}$	465	93%
$N_{det\ \subset S_{spoof}}$	17	3,4%
$N_{det\ \notin S_{spoof}}$	18	3,6%
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	0	0,0%

$P_{sygn\ [\sim det | \in S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	13	2,6%
2	2	0,4%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	2	0,4%
7	—	—
8	—	—

$P_{sygn\ [\in S_{spoof} | \notin S_{spoof}]}$

N_{sygn}	N_{wyst}	Udział
1	0	0,0%
2	18	3,6%
3	0	0,0%
4	0	0,0%
5	0	0,0%
6	0	0,0%

Parametry jakościowe detekcji i eliminacji spoofingu dla scenariusza IV_C_6 przedstawiono w Tab. 6.27 i 6.28. W tym scenariuszu wystąpiły przypadki niewykrycia części transmitowanych sygnałów fałszywych. Stanowią one 3,4% wszystkich pomiarów. W podobnej liczbie przypadków wystąpiło uznanie dwóch sygnałów prawdziwych za sygnały spoofera. W dwóch pomiarach

(0,4% przypadków) spoofing nie został wykryty, gdyż pierwsza akwizycja nie znalazła żadnego sygnału o numerze spośród numerów sygnałów fałszywych. Należy zwrócić uwagę, że odsetek poprawnych detekcji spoofingu, wynoszący 93%, jest nadal stosunkowo wysoki. Można zatem stwierdzić, że warunki propagacji wielodrogowej nie powodują znaczącego pogorszenia efektywności wykrywania spoofingu.

Tabela 6.28: Parametry jakościowe eliminacji spoofingu w scenariuszu IV_C_6

$\overline{\frac{C}{N_0}}_{\in S_{spoof}}$	51,2 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}}$	38,9 dBHz
$\overline{\frac{C}{N_0}}_{\in S_{spoof\ \ filtr}}$	45,4 dBHz
$\overline{\frac{C}{N_0}}_{\notin S_{spoof\ \ filtr}}$	41,2 dBHz

$P_{\notin S_{spoof}}$			$P_{\notin S_{spoof\ \ filtr}}$		
N_{sygn}	N_{wyst}	Udział	N_{sygn}	N_{wyst}	Udział
0	378	75,6%	0	66	13,2%
1	104	20,8%	1	94	18,8%
2	18	3,6%	2	112	22,4%
3	0	0,0%	3	138	27,6%
4	0	0,0%	4	71	14,2%
5	0	0,0%	5	19	3,8%
6	0	0,0%	6	0	0,0%

Spadek średniej wartości $\frac{C}{N_0}$ sygnałów spoofera, wywołany filtracją przestrzenną, wynosi 5,8 dB. Ta wartość po filtracji jest równa 45,4 dBHz, co oznacza, że w dalszym ciągu są to stosunkowo silne sygnały, które mogą znacząco utrudniać odbiór sygnałów pochodzących z satelitów. Słabsze wytłumienie sygnałów spoofera skutkuje mniejszym wzrostem średniej wartości $\frac{C}{N_0}$ sygnałów prawdziwych, który wynosi w tym przypadku jedynie 2,3 dB. Jest to jedyny, spośród analizowanych scenariuszy, w którym, po filtracji przestrzennej, wartość $\frac{C}{N_0}$ sygnałów prawdziwych (41,2 dBHz) jest mniejsza od wartości $\frac{C}{N_0}$ sygnałów fałszywych. Wynika stąd, że proces eliminacji spoofingu jest znacznie bardziej wrażliwy na występowanie propagacji wielodrogowej, niż proces detekcji.

Pomimo jedynie częściowego stłumienia sygnałów spoofera, można zauważyć korzystny wpływ filtracji przestrzennej na możliwość odbioru sygnałów z satelitów GPS. Przed filtracją w 75,6% przypadków nie był możliwy odbiór żadnego z tych sygnałów, podczas gdy po filtracji w 45,6% przypadków można było odbierać co najmniej trzy.

6.6 Podsumowanie wyników badań pomiarowych

Przedstawione w niniejszym rozdziale wyniki badań pomiarowych są podstawą do dokonania oceny działania systemu antyspoofingowego w postaci zaproponowanej w niniejszej rozprawie doktorskiej.

Rezultaty pierwszego etapu pomiarów stanowią potwierdzenie wyników badań symulacyjnych, dotyczących wykrywania spoofingu. Weryfikują one zależności pomiędzy wartością stosunku $\frac{C}{N_0}$ i liczbą odbieranych fałszywych sygnałów a prawdopodobieństwem detekcji spoofingu. Dowodzi to wysokiej skuteczności wykrywania w warunkach odbioru sygnałów fałszywych o dużej mocy, transmitowanych w kanale AWGN (z addytywnym białym szumem gaussowskim).

Wyniki uzyskane w drugim etapie umożliwiły wstępną ewaluację procedury eliminacji spoofingu w ustalonych warunkach laboratoryjnych. Zgodnie z oczekiwaniami, stwierdzono wytłumienie sygnałów fałszywych. Odnotowano także, związaną z tym, poprawę jakości odbioru wytworzonego lokalnie sygnału testowego, pełniącego rolę pojedynczego sygnału prawdziwego o zmiennej mocy.

Pomiary wykonane w trzecim etapie wykazały, że proponowane sposobu wykrywania i eliminacji spoofingu skutecznie przywracają możliwość odbioru sygnałów pochodzących z satelitów GPS, w przypadku gdy, w miejscu odbioru, te sygnały są zagłuszone przez sygnały pochodzące ze spoofera, przesyłane w kanale AWGN.

W etapie czwartym uwzględniono wpływ charakterystyk kanału radiowego, pomiędzy spooferem a odbiornikiem, na skuteczność przeciwdziałania spoofingowi. W scenariuszach, w których nie występowało zjawisko propagacji wielodrogowej, efektywność eliminacji spoofingu była zbliżona do tej, którą zaobserwowano w etapie III. Z kolei analizując parametry detekcji spoofingu, wykryto przypadki nieprawidłowego określenia numerów fałszywych sygnałów. Nie było to jednak spowodowane odmienną charakterystyką kanału transmisyjnego, lecz zmniejszeniem mocy sygnałów spoofera w stosunku do sygnałów prawdziwych. Możliwość wykrycia niektórych sygnałów prawdziwych jeszcze przed eliminacją spoofingu sprawia, że mogą one zostać uznane za fałszywe, jeśli związane z nimi różnice opóźnień fazowych są mniejsze niż próg detekcji. Jest to szczególnie prawdopodobne wtedy, gdy próg detekcji jest duży. Na podstawie dodatko-

wych badań pomiarowych, dowiedziono, że zmniejszenie progów detekcji spoofingu umożliwia poprawę identyfikacji numerów fałszywych sygnałów. Należy jednak mieć na uwadze, że taka modyfikacja zmniejsza prawdopodobieństwo detekcji w przypadku fałszywych sygnałów o małych wartościach $\frac{C}{N_0}$.

Ostatnia część pomiarów wykonanych w etapie IV dotyczyła warunków badań efektywności wykrywania i eliminacji spoofingu w warunkach transmisji sygnałów spoofera przez kanał charakteryzujący się propagacją wielodrogową. Stwierdzono, że w takich warunkach nadal jest możliwe uzyskanie stosunkowo wysokiej efektywności wykrywania. Odnotowano jednakże istotne pogorszenie eliminacji spoofingu, co wynika z przyjętego sposobu filtracji przestrzennej, w której tłumione są sygnały niepożądane docierające tylko z jednego kierunku.

Podsumowanie

Spoofing GNSS, stanowi potencjalne poważne zagrożenie dla bezpieczeństwa urządzeń i systemów, które korzystają z informacji zawartych w sygnałach nadawanych przez satelity globalnych systemów nawigacyjnych. Realizacja tego typu ataków może być szczególnie niebezpieczna w obszarach takich jak m.in.: nawigacja (lądowa, morska, lotnicza i kosmiczna), energetyka czy telekomunikacja. Podatność, dostępnych na rynku, cywilnych odbiorników GPS na spoofing została potwierdzona w wielu niezależnych badaniach, w tym w projekcie badawczo rozwojowym, którego wykonawcą był doktorant. Wniosek płynący z tych badań jest taki, że, jeśli nie zostaną podjęte niezbędne kroki w celu zapewnienia odpowiedniej ochrony odbiorników nawigacyjnych, systemy nawigacji satelitarnej GNSS nie powinny być używane jako jedyne źródło informacji o położeniu, prędkości i czasie w tzw. aplikacjach krytycznych.

Analizując dotychczas opublikowane propozycje sposobów przeciwdziałania spoofingowi w systemie GPS, można stwierdzić, że nie reprezentują one kompleksowych rozwiązań, umożliwiających zarówno wykrycie obecności spoofingu, jak i jego eliminację. Większość z proponowanych metod charakteryzuje się ograniczoną efektywnością w przypadku bardziej zaawansowanych scenariuszy spoofingu. Spośród czynników, które umożliwiają odróżnienie fałszywych i prawdziwych sygnałów GPS, najbardziej jednoznacznym i najtrudniejszym do sfałszowania jest kierunek nadejścia sygnału i jego pochodne. Metody wykrywania spoofingu, bazujące na innych parametrach sygnałów, są zwykle łatwiejsze w implementacji, jednakże mogą być nieefektywne w przypadku bardziej zaawansowanych spooferów.

W niniejszej pracy zaproponowano koncepcję systemu antyspoofingowego, która obejmuje metodę wykrywania transmisji fałszywych sygnałów GPS oraz metodę ich eliminacji w odbiorniku. Obie one bazują na autorskich algorytmach przestrzennego przetwarzania sygnałów. Innowację stanowi m.in. przyjęte kryterium odróżniania sygnałów prawdziwych od fałszywych. Tym kryterium są różnice wartości opóźnień fazowych fal nośnych tych sygnałów. Opóźnienia te są mierzone pomiędzy wybranymi elementami odbiorczego szyku antenowego i są ściśle związane z kierunkiem nadejścia sygnału, który w praktyce nie może zostać sfałszowany przez spoofer.

Znajomość dokładnych opóźnień fazowych sygnałów fałszywych umożliwia nie tylko wykrycie spoofingu, lecz również selektywne wyeliminowanie tych sygnałów z całego sygnału odbieranego, przy użyciu algorytmu kształtowania zer (ang. null-steering). Opracowany przez autora system antyspoofingowy, w którym algorytm eliminacji spoofingu bazuje na parametrach sygnału wyznaczonych podczas detekcji spoofingu, ma charakter oryginalny. W dotychczasowych publikacjach metody wykrywania i eliminacji spoofingu były rozpatrywane oddzielnie.

Efektywność zaproponowanych metod antyspoofingowych została określona na drodze badań symulacyjnych i pomiarowych. Pierwsze z wymienionych miały na celu zbadanie funkcjonowania tych rozwiązań w modelowych warunkach transmisji. Wyniki symulacji stanowią punkt odniesienia dla późniejszej oceny pracy systemu antyspoofingowego w warunkach rzeczywistych. W trzech etapach badań symulacyjnych, związanych z wykrywaniem spoofingu, określono kolejno: charakterystyki błędu estymacji opóźnień fazowych, wartości progów detekcji spoofingu przy dopuszczalnym prawdopodobieństwie fałszywego alarmu oraz krzywe prawdopodobieństwa detekcji w zależności od liczby fałszywych sygnałów i ich jakości. W symulacjach dotyczących eliminacji spoofingu wyznaczono możliwe do uzyskania wartości tłumienia sygnałów fałszywych. Przeanalizowano także metodę poprawy tłumienia tych sygnałów w przypadku wyznaczenia niedokładnych opóźnień fazowych. Ponadto, określono wpływ zastosowania przestrzennej filtracji sygnałów na możliwości odbioru sygnałów z satelitów GPS.

Wyniki przeprowadzonych badań symulacyjnych wstępnie potwierdziły zasadność stosowania opracowanych metod antyspoofingowych. Kolejnym etapem prac było zweryfikowanie ich działania w warunkach rzeczywistych. W tym celu zostało zbudowane stanowisko pomiarowe,

którego głównym elementem jest prototyp systemu antyspoofingowego, zrealizowany w technice radia programowalnego. Pomiary zostały przeprowadzone w czterech etapach, przy użyciu różnych konfiguracji stanowiska badawczego, przy czym kolejne konfiguracje odzwierciedlały warunki coraz bardziej zbliżone do rzeczywistego scenariusza spoofingu. Wyniki badań pomiarowych w pierwszym etapie potwierdziły, uzyskane uprzednio w drodze symulacji, charakterystyki błędu estymacji opóźnień fazowych oraz charakterystyki prawdopodobieństwa wykrycia spoofingu przy ustalonych progach detekcji.

Drugi etap badań pomiarowych miał na celu generalną weryfikację działania algorytmu filtracji przestrzennej, jako metody eliminacji sygnałów spoofera przy zachowaniu możliwości odbioru sygnałów prawdziwych. Uzyskane wyniki potwierdziły poprawność implementacji algorytmu kształtowania zer.

Zasadniczą część badań pomiarowych stanowią te przeprowadzone w etapach III i IV. Na podstawie ich wyników było możliwe dokonanie całościowej oceny pracy systemu antyspoofingowego. W przypadku użycia konfiguracji III stanowiska badawczego, w której fałszywe sygnały o dużej mocy były przesyłane medium przewodowym, działanie systemu było wzorcowe. Algorytm detekcji w każdym przypadku wykrywał obecność spoofingu i określał zbiór fałszywych sygnałów. Natomiast w wyniku filtracji przestrzennej fałszywe sygnały zostały praktycznie zupełnie wyeliminowane i uzyskano możliwość odbioru sygnałów prawdziwych zbliżoną do takiej, jaka występuje przy braku spoofingu.

Przy użyciu konfiguracji IV stanowiska, która reprezentuje spoofing w warunkach rzeczywistych, zidentyfikowano czynniki, które wpływają negatywnie na efektywność wykrywania i eliminacji spoofingu. Pierwszym z nich jest zbyt mała różnica mocy odbieranych sygnałów fałszywych i prawdziwych. W założeniach badań symulacyjnych przyjęto, że moc sygnałów spoofera jest na tyle duża, że całkowicie uniemożliwia prawidłowy odbiór sygnałów z satelitów GPS. Zgodnie z tym założeniem wyznaczono wartości progów detekcji spoofingu. Równoczesny odbiór sygnałów prawdziwych i fałszywych pogarsza działanie algorytmu detekcji, z uwagi na możliwość uznania sygnału prawdziwego za fałszywy. Taka błędna decyzja jest w tym przypadku znacznie bardziej prawdopodobna niż wtedy, gdy spoofing nie występuje. Biorąc pod

uwagę możliwość wykrycia sygnałów prawdziwych jeszcze przed eliminacją spoofingu, np. gdy odbiornik znajduje się daleko od spoofera, jest konieczne zmniejszenie wartości progów detekcji. W punkcie 6.5.2 wykazano, że ograniczenie maksymalnych wartości progów detekcji wpływa korzystnie na poprawność identyfikacji numerów fałszywych sygnałów. Kosztem obniżenia progów detekcji jest zmniejszenie prawdopodobieństwa wykrycia spoofingu przy małych wartościach $\frac{C}{N_0}$ sygnałów spoofera. Propozycją innego rozwiązania problemu równoczesnego odbioru sygnałów prawdziwych i fałszywych może być zastosowanie pomocniczo algorytmu RAIM, który stwierdzi, czy wyznaczony zbiór fałszywych sygnałów jest spójny pod względem depesz nawigacyjnych i pseudoodległości. Sygnały prawdziwe, stanowiące mniejszość w tym zbiorze, powinny zostać odrzucone.

Drugim z czynników, warunkujących poprawność działania rozważanego systemu antyspoofingowego w warunkach rzeczywistych, jest intensywność propagacji wielodrogowej w kanale radiowym pomiędzy spooferem a odbiornikiem GPS. Przyjęty w rozprawie sposób realizacji filtru przestrzennego umożliwia silne stłumienie sygnałów docierających z jednego kierunku, określonego wartościami opóźnień fazowych fal nośnych. W sytuacji gdy sygnał dociera do odbiornika wieloma drogami, blokowany jest wyłącznie odbiór najsilniejszej składowej i ewentualnych innych sygnałów nadchodzących z tego samego kierunku. Jeśli co najmniej jedna z pozostałych składowych przestrzennych sygnału odbieranego ma stosunkowo dużą moc, odbiór sygnałów z satelitów GPS może być utrudniony. Równoczesna eliminacja sygnałów docierających z różnych kierunków jest możliwa przy zastosowaniu takiej postaci wektora wag filtracji przestrzennej, w której charakterystyka odbiorcza ma wiele zer. Jeśli szyk antenowy jest zbudowany z M elementów, jest możliwe stłumienie sygnałów z maksymalnie $M-1$ kierunków (vide Rys.2.3). W takim przypadku jest konieczne wyznaczenie zestawów opóźnień fazowych niezależnie dla każdej składowej przestrzennej sygnału spoofera. Niedogodnością ustalania wielu zer charakterystyki odbiorczej szyku antenowego jest to, że takie zera są bardziej rozproszone przestrzennie i, w związku z tym, mogą być również tłumione sygnały prawdziwe, nadchodzące z innych kierunków niż sygnały spoofera.

Reasumując, poprzez przeprowadzone analizy i badania wykazano słuszność tezy postawionej w pierwszym rozdziale tej rozprawy doktorskiej:

Przy zastosowaniu odbioru wieloantenowego jest możliwe wykrycie spoofingu GPS, polegającego na emisji imitacji sygnałów systemu GPS przez urządzenie zwane spooferem. Ponadto, poprzez zastosowanie filtracji przestrzennej, jest możliwe ograniczenie wpływu sygnałów nadawanych przez spoofer na pracę odbiornika GPS.

Wskazana jest kontynuacja opisanych badań, mająca na celu określenie możliwości uniezależnienia efektywności wykrywania i eliminacji spoofingu od warunków propagacyjnych w kanale pomiędzy spooferem a odbiornikiem. Rozwiązania wymagają, w szczególności, kwestie propagacji wielodrogowej oraz równoczesnego odbioru sygnałów prawdziwych i fałszywych.

Do najważniejszych autorskich osiągnięć niniejszej rozprawy doktorskiej można zaliczyć:

1. Zaproponowanie nowej metody detekcji spoofingu GPS, bazującej na analizie różnic opóźnień fazowych fal nośnych odbieranych sygnałów GPS.

2. Zastosowanie algorytmu kształtowania zer charakterystyki odbiorczej jako metody eliminacji fałszywych sygnałów, bazującej na parametrach wyznaczanych na etapie detekcji spoofingu.

3. Na podstawie powyższych - opracowanie koncepcji kompleksowego systemu antyspoofingowego, łączącego opracowaną metodę wykrywania spoofingu z wybraną metodą jego eliminacji. Koncepcja precyzuje m.in. zasady działania obu metod oraz określa umiejscowienie bloków systemu antyspoofingowego w odniesieniu do schematu funkcjonalnego standardowego odbiornika GPS.

4. Zdefiniowanie parametrów umożliwiających ocenę efektywności różnych metod wykrywania i eliminacji spoofingu.

5. Opracowanie i przeprowadzenie badań symulacyjnych, służących wyznaczeniu m.in. prawdopodobieństwa detekcji spoofingu, osiągalnego tłumienia sygnałów spoofera oraz wpływu eliminacji spoofingu na możliwość odbioru sygnałów prawdziwych.

6. Zaprojektowanie i zbudowanie prototypu systemu antyspoofingowego w technice radia programowalnego, na podstawie opracowanej koncepcji.

7. Opracowanie i przeprowadzenie oryginalnych badań pomiarowych z użyciem stanowiska badawczego, którego głównym elementem jest zrealizowany prototyp.

8. Przeanalizowanie wyników pomiarów pod kątem weryfikacji badań symulacyjnych oraz dokonania całościowej oceny efektywności opracowanego systemu antyspoofingowego.

Wybrane wyniki prac realizowanych w ramach doktoratu zostały opublikowane na łamach czasopism naukowych (m.in. w [61, 62, 63, 64]), a także zaprezentowane na konferencjach międzynarodowych (m.in. [56, 57, 59]) i krajowych (m.in. [58, 60]). Podjęto również działania mające na celu uzyskanie ochrony patentowej opracowanych rozwiązań [44].

Bibliografia

[1] 2J Antennae. *GNSS module with pre-filter.* Specyfikacja techniczna, http://www.2j-antennae.com/images/products/2J401F-GF.pdf. [cytowanie na str. 87]

[2] T.W. Anderson, D.A. Darling. Asymptotic Theory of Certain "Goodness of Fit" Criteria Based on Stochastic Processes. *The Annals of Mathematical Statistics*, wol. 23 (nr 2), s. 193–212, 1952. [cytowanie na str. 67]

[3] A. T. Balaei, B. Motella, A. Dempster. A preventative approach to mitigating CW interference in GPS receivers. *GPS Solutions*, wol. 12 (nr 4), s. 199–209, 2008. [cytowanie na str. 10]

[4] A.T. Balaei, J. Barnes, A.G. Dempster. Characterization of interference effects on GPS signal carrier phase error. *SSC 2005 Spatial Intelligence, Innovation and Praxis: The national biennial Conference of the Spatial Science Institute*, 2005. [cytowanie na str. 64]

[5] A.T. Balaei, A.G. Dempster, D. Akos. Quantization Degradation of GNSS Signal Quality in the Presence of CW RFI. *Spread Spectrum Techniques and Applications, 2008. ISSSTA '08. IEEE 10th International Symposium on*, , s. 42–47, 2008. [cytowanie na str. 25]

[6] A.T. Balaei, A.G. Dempster, L. Lo Presti. Characterization of the Effects of CW and Pulse CW Interference on the GPS Signal Quality. *Aerospace and Electronic Systems, IEEE Transactions on*, wol. 45 (nr 4), s. 1418–1431, 2009. [cytowanie na str. 54]

[7] J. Bao-Yen Tsui. *Fundamentals of Global Positioning System Receivers: A Software Approach.* Wiley Series in Microwave and Optical Engineering. Wiley, 2005. [cytowanie na str. 40]

[8] A. Bensky. *Wireless Positioning Technologies and Applications.* Artech House, 2007. [cytowanie na str. 37]

[9] A. Brown. Performance and jamming test results of a digital beamforming GPS receiver. http://www.navsys.com/papers/0205002.pdf, NAVSYS Corporation, 2002. [cytowanie na str. 30]

[10] A. Brown, B. Mathews. Constrained Beamforming for Space GPS Navigation. http://www.navsys.com/papers/07-09-001.pdf, NAVSYS Corporation. [cytowanie na str. 84]

[11] A. Brown, H. Tseng. Miniaturized GPS Antenna Array and Test Results. http://www.navsys.com/papers/0005002.pdf, NAVSYS Corporation, 2006. [cytowanie na str. 56]

[12] A.K. Brown, B. Mathews. GPS Multipath Mitigation Using a Three Dimensional Phased Array. *18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005)*, , s. 659 – 666, 2005. Long Beach, USA. [cytowanie na str. 56]

[13] A. Cavaleri, B. Motella, M. Pini, M. Fantino. Detection of spoofed GPS signals at code and carrier tracking level. *Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 2010 5th ESA Workshop on*, , s. 1–6, 2010. [cytowanie na str. 21]

[14] X. Chen, F. Dovis, M. Pini, P. Mulassano. Turbo architecture for multipath mitigation in global navigation satellite system receivers. *Radar, Sonar Navigation, IET*, wol. 5 (nr 5), s. 517–527, 2011. [cytowanie na str. 21]

[15] Z. Chen, G. Gokeda, Y. Yu. *Introduction to Direction-of-Arrival Estimation*. Artech House Signal Processing Library. Artech House, 2010. [cytowanie na str. 56]

[16] X. Cheng, J. Xu, K. Cao, J. Wang. An Authenticity Verification Scheme Based on Hidden Messages for Current Civilian GPS Signals. *Computer Sciences and Convergence Information Technology, 2009. ICCIT '09. Fourth International Conference on*, , s. 345–352, 2009. [cytowanie na str. 22]

[17] M. Cuntz, L. Greda, M. Heckler, A. Konovaltsev, M. Meurer. Lessons Learnt: The Development of a Robust Multi-Antenna GNSS Receiver. *ION GNSS 2010*, , s. 2852–2859, 2010. [cytowanie na str. 56]

[18] M. Cuntz, A. Konovaltsev, A. Dreher, M. Meurer. Jamming and Spoofing in GPS/GNSS Based Applications and Services - Threats and Countermeasures. *Future Security*, 318 serii *Communications in Computer and Information Science*, , s. 196–199. Springer, 2012. [cytowanie na str. 30]

[19] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, G. Lachapelle. A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array. *25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, , s. 1233 – 1243, 2012. [cytowanie na str. 29]

[20] D.A. Divis. GPS Spoofing Experiment Knocks Ship off Course (http://www.insidegnss.com/node/3659), 2013. [cytowanie na str. 14]

[21] F. Dovis, X. Chen, A. Cavaleri, K. Ali, M. Pini. Detection of spoofing threats by means of signal parameters estimation. *24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, , s. 416–421, 2001. [cytowanie na str. 21]

[22] F. Dovis, L. Musumeci. Use of Wavelet transforms for interference mitigation. *Localization and GNSS (ICL-GNSS), 2011 International Conference on*, , s. 116–121, 2011. [cytowanie na str. 24]

[23] EttusResearch. *USRP Hardware Driver™ software*. Strona WWW projektu: http://code.ettus.com/redmine/ettus/projects/uhd/wiki/. [cytowanie na str. 91]

[24] E. Falletti, M. Pini, L. Lo Presti, D. Margaria. Assessment on low complexity C/No estimators based on M-PSK signal model for GNSS receivers. *Position, Location and Navigation Symposium, 2008 IEEE/ION*, , s. 167–172, 2008. [cytowanie na str. 51]

[25] E. Falletti, M. Pini, L.L. Presti. Are Carrier-to-Noise Algorithms Equivalent in All Situations? *Inside GNSS*, (nr 01-02), s. 20–27, 2010. [cytowanie na str. 50]

[26] E. Falletti, M. Pini, L.L. Presti. Low Complexity Carrier-to-Noise Ratio Estimators for GNSS Digital Receivers. *Aerospace and Electronic Systems, IEEE Transactions on*, wol. 47 (nr 1), s. 420–437, 2011. [cytowanie na str. 50]

[27] C. Fernandez-Prades, P. Closas, J. Arribas. Eigenbeamforming for interference mitigation in GNSS receivers. *Localization and GNSS (ICL-GNSS), 2011 International Conference on*, , s. 93–97, 2011. [cytowanie na str. 30]

[28] Z. Fu, A. Hornbostel, J. Hammesfahr, A. Konovaltsev. Suppression of multipath and jamming signals by digital beamforming for GPS/Galileo applications. *GPS Solutions*, wol. 6 (nr 4), s. 257–264, 2003. [cytowanie na str. 30]

[29] Global Positioning System Directorate. *Interface Specification IS-GPS-200G*, 2012. http://www.gps.gov/technical/icwg/IS-GPS-200G.pdf. [cytowanie na str. 9, 11, 22]

[30] Mapy Google. https://www.google.pl/maps/. [cytowanie na str. 119, 132]

[31] P.D. Groves. *Principles of GNSS, Inertial, and Multisensor Integrated Navigation Systems*. GNSS technology and applications series. Artech House, 2008. [cytowanie na str. 22]

[32] G.F. Hatke. Adaptive array processing for wideband nulling in GPS systems. *Signals, Systems amp; Computers, 1998. Conference Record of the Thirty-Second Asilomar Conference on*, wol. 2, , s. 1332–1336, 1998. [cytowanie na str. 30]

[33] G. Hein, F. Kneissl, J.A. Avila-Rodriguez, S. Wallner. Authenticating GNSS: Proofs against spoofs. *Inside GNSS*, wol. 2 (nr 4), s. 58–63, 2007. [cytowanie na str. 22]

[34] B. Hofmann-Wellenhof, H. Lichtenegger, E. Wasle. *GNSS – Global Navigation Satellite Systems: GPS, GLONASS, Galileo, and more*. Springer Vienna, 2007. [cytowanie na str. 6]

[35] T.E. Humphreys, B.M. Ledvina, M.L. Psiaki, B.W. O'Hanlon, P.M. Kintner Jr. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. *ION GNSS international technical meeting of the satellite division*, wol. 55, 2008. [cytowanie na str. 26]

[36] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, G. Lachapelle. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *International Journal of Navigation and Observation*, wol. 2012. doi:10.1155/2012/127072. [cytowanie na str. 12, 18]

[37] X. Jiang, J. Zhang, B.J. Harding, J.J. Makela, A.D. Dominguez-Garcia. Spoofing GPS Receiver Clock Offset of Phasor Measurement Units. *Power Systems, IEEE Transactions on*, wol. 28 (nr 3), s. 3253–3262, 2013. [cytowanie na str. 14]

[38] G.W. Johnson, P.F. Swaszek, R.J. Hartnett, R. Shalaev, M. Wiggins. An Evaluation of eLoran as a Backup to GPS. *Technologies for Homeland Security, 2007 IEEE Conference on*, , s. 95–100, 2007. [cytowanie na str. 22]

[39] J.C. Juang. GNSS spoofing analysis by VIAS. *Coordinates Magazine*, (nr 1), 2011. http://mycoordinates.org/gnss-spoofing-analysis-by-vias/. [cytowanie na str. 19]

[40] E. Kaplan, C. Hegarty. *Understanding GPS: Principles and Applications, Second Edition*. Artech House mobile communications series. Artech House, 2005. [cytowanie na str. 8]

[41] G. Kappen, C. Haettich, M. Meurer. Towards a robust multi-antenna mass market GNSS receiver. *Position Location and Navigation Symposium (PLANS), 2012 IEEE/ION*, , s. 291–300, 2012. [cytowanie na str. 56]

[42] R.S. Kashyap, R. Bhide, V. Ganwani. Adaptive Beamforming for Multi-path Mitigation in GPS. Course project report, Indian Institute of Technology, Bombay. [cytowanie na str. 30]

[43] R. Katulski, A. Białowąs, K. Bronk, K. Dymarkowski, J. Garus, J. **Magiera**, R. Namiotko, B. Rauhut-Sobczak, J. Stefański, A. Czapiewska, R. Studański, R. Wąs, R. Zając. Raport z realizacji projektu badawczego rozwojowego NCBiR nr OR 0000808 pn. Demonstrator technologii zakłócania transmisji radiowych z widmem rozproszonym DS CDMA. , Politechnika Gdańska, 2011. [cytowanie na str. 1]

[44] R. Katulski, J. **Magiera**, J. Stefański, A. Studańska. Układ do spoofingu realizowanego w systemach nawigacji satelitarnej. Zgłoszenie patentowe UPRP nr P.395689. [cytowanie na str. 156]

[45] R. Katulski, J. **Magiera**, J. Stefański, A. Studańska. Badania odporności na zakłócenia wybranych systemów GNSS. *Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne*, (nr 6), 2011. [cytowanie na str. 9]

[46] R. Katulski, J. **Magiera**, J. Stefański, A. Studańska. Research study on reception of GNSS signals in presence of intentional interference. *Telecommunications and Signal Processing (TSP), 2011 34th International Conference on*, , s. 452–456, 2011. [cytowanie na str. 10]

[47] R. Katulski, J. **Magiera**, A. Studańska. Device for spoofing in Global Positioning System. *Zeszyty Naukowe Akademii Marynarki Wojennej*, wol. 53 (nr 4 (191)), s. 63–70, 2012. [cytowanie na str. 13]

[48] A. J. Kerns, D. P. Shepard, J. A. Bhatti, T. E. Humphreys. Unmanned Aircraft Capture and Control Via GPS Spoofing. *Journal of Field Robotics*, wol. 31 (nr 4), s. 617–636, 2014. [cytowanie na str. 14]

[49] S. Kim, R.A Iltis. GPS C/A code tracking with adaptive beamforming and jammer nulling. *Signals, Systems and Computers, 2002. Conference Record of the Thirty-Sixth Asilomar Conference on*, wol. 2, , s. 975–979, 2002. [cytowanie na str. 30]

[50] J.A. Klobuchar. Ionospheric Time-Delay Algorithm for Single-Frequency GPS Users. *Aerospace and Electronic Systems, IEEE Transactions on*, wol. AES-23 (nr 3), s. 325–331, 1987. [cytowanie na str. 20]

[51] M. Kuhn. An Asymmetric Security Mechanism for Navigation Signals. *Information Hiding Workshop*, , s. 239–252. Springer, 2004. [cytowanie na str. 22]

[52] B. Ledvina, P. Montgomery, T. Humphreys. A Multi-Antenna Defense: Receiver-Autonomous GPS Spoofing Detection. *Inside GNSS*, (nr 03-04), s. 40–46, 2009. [cytowanie na str. 12, 55]

[53] B.M. Ledvina, W.J. Bencze, B. Galusha, I. Miller. An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers. *2010 International Technical Meeting of The Institute of Navigation*, , s. 698–712, 2010. San Diego, USA. [cytowanie na str. 12]

[54] M. Li, A.G. Dempster, A.T. Balaei, C. Rizos, F. Wang. Switchable Beam Steering/Null Steering Algorithm for CW Interference Mitigation in GPS C/A Code Receivers. *Aerospace and Electronic Systems, IEEE Transactions on*, wol. 47 (nr 3), s. 1564–1579, 2011. [cytowanie na str. 31]

[55] J. **Magiera**. Analiza porównawcza systemów nawigacji satelitarnej GPS i GLONASS. *Przegląd Telekomunikacyny i Wiadomości Telekomunikacyjne*, (nr 2-3), s. 72–76, 2010. [cytowanie na str. 37]

[56] J. **Magiera**. Design and implementation of GPS signal simulator. *Localization and GNSS (ICL-GNSS), 2012 International Conference on*, 2012. [cytowanie na str. 12, 156]

[57] J. **Magiera**, R. Katulski. Accuracy of differential phase delay estimation for GPS spoofing detection. *Telecommunications and Signal Processing (TSP), 2013 36th International Conference on*, , s. 695–699, 2013. Rzym, Włochy. [cytowanie na str. 156]

[58] J. **Magiera**, R. Katulski. Analiza dokładności wyznaczania różnicowych opóźnień fazowych w systemie wykrywania spoofingu GPS. *Przegląd Telekomunikacyny i Wiadomości Telekomunikacyjne (Krajowa Konferencja Radiokomunikacji, Radiofonii i Telewizji 2013, Wrocław, 10-12.06.2013)*, (nr 6), s. 452–455, 2013. [cytowanie na str. 156]

[59] J. **Magiera**, R. Katulski. Applicability of Null-Steering for Spoofing Mitigation in Civilian GPS. *Vehicular Technology Conference (VTC Spring), 2014 IEEE 79th*, 2014. Seul, Korea Płd. [cytowanie na str. 156]

[60] J. **Magiera**, R. Katulski. Efektywność filtracji przestrzennej sygnałów w przeciwdziałaniu spoofingowi GPS. *Przegląd Telekomunikacyny i Wiadomości Telekomunikacyjne (Krajowa Konferencja Radiokomunikacji, Radiofonii i Telewizji 2014, Warszawa, 11-13.06.2014)*, (nr 6), s. 294–297, 2014. [cytowanie na str. 156]

[61] J. **Magiera**, R. Katulski. Technika ochrony odbiorników GPS przed atakami typu spoofing. *Przegląd Komunikacyjny*, (nr 11), s. 19–21, 2014. [cytowanie na str. 156]

[62] J. **Magiera**, R. Katulski. Analiza i badania systemu antyspoofingowego GPS. *Przegląd Elektrotechniczny*, wol. 91 (nr 3), s. 66–69, 2015. [cytowanie na str. 156]

[63] J. **Magiera**, R. Katulski. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *Journal of Applied Research and Technology (**JCR**)*, wol. 13 (nr 1), s. 45–57, 2015. [cytowanie na str. 156]

[64] J. **Magiera**, R. Katulski. Metody ochrony przed spoofingiem w systemach nawigacji satelitarnej GNSS. *Przegląd Telekomunikacyny i Wiadomości Telekomunikacyjne*, (nr 1), s. 5–10, 2015. [cytowanie na str. 156]

[65] S. Matelski, K. Matti, M. Mienik, M. Pacuszka, J. Pindelski. Elektronicznie sterowany statyw do układu antenowego GPS. Dokumentacja techniczna projektu grupowego, Politechnika Gdańska, Wydział ETI, 2014. Opiekun projektu: J. **Magiera**. [cytowanie na str. 87]

[66] M. Meurer, A. Konovaltsev, M. Cuntz, C. Hättich. Robust Joint Multi-Antenna Spoofing Detection and Attitude Estimation using Direction Assisted Multiple Hypotheses RAIM. *25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, , s. 3007 – 3016, 2012. Nashville, USA. [cytowanie na str. 21]

[67] Mini Circuits. *Coaxial bandpass filter VBF-1575+*. Specyfikacja techniczna, http://minicircuits.com/pdfs/VBF-1575+.pdf. [cytowanie na str. 88]

[68] Mini Circuits. *Coaxial bias-tee ZFBT-352-FT+*. Specyfikacja techniczna, http://minicircuits.com/pdfs/ZFBT-352-FT+.pdf. [cytowanie na str. 88]

[69] Mini Circuits. *Connectorized amplifier ZX60-2534M+*. Specyfikacja techniczna, http://minicircuits.com/pdfs/ZX60-2534M+.pdf. [cytowanie na str. 89]

[70] R.H. Mitch. Signal Characteristics of Civil GPS Jammers. *ION GNSS, Portland, Oregon, 2011*, 2011. [cytowanie na str. 10]

[71] B. Motella, M. Pini, F. Dovis. Investigation on the effect of strong out-of-band signals on global navigation satellite systems receivers. *GPS Solutions*, wol. 12 (nr 2), s. 77–86, 2008. [cytowanie na str. 11]

[72] National Instruments. *NI USRP-292x/293x Datasheet - Universal Software Radio Peripherals.* Specyfikacja tehcniczna, http://www.ni.com/datasheet/pdf/en/ds-355. [cytowanie na str. 89]

[73] J. Nielsen, A. Broumandan, G. Lachapelle. Spoofing detection and mitigation with a moving handheld receiver. *GPS World*, (nr 09), s. 27–33, 2010. [cytowanie na str. 21]

[74] A. Noureldin, T.B. Karamat, M.D. Eberts, A. El-Shafie. Performance Enhancement of MEMS-Based INS/GPS Integration for Low-Cost Navigation Applications. *Vehicular Technology, IEEE Transactions on*, wol. 58 (nr 3), s. 1077–1096, 2009. [cytowanie na str. 22]

[75] P. Papadimitratos, A. Jovanovic. GNSS-based positioning: Attacks and countermeasures. *Military Communications Conference, 2008. MILCOM 2008. IEEE*, , s. 1–7. IEEE, 2008. [cytowanie na str. 22]

[76] R.E. Phelts. *Multicorrelator Techniques for Robust Mitigation of Threats to GPS Signal Quality.* Praca doktorska, Stanford University, 2001. [cytowanie na str. 21]

[77] R.E. Phelts, D.M. Akos, P. Enge. Robust signal quality monitoring and detection of evil waveforms. *13th International Technical Meeting of the Satellite Division of the Institute of Navigation*, 2000. [cytowanie na str. 21]

[78] M. Pini, E. Falletti, M. Fantino. Performance Evaluation of C/N0 Estimators Using a Real Time GNSS Software Receiver. *Spread Spectrum Techniques and Applications, 2008. ISSSTA '08. IEEE 10th International Symposium on*, , s. 28–31, 2008. [cytowanie na str. 51]

[79] O. Pozzobon. Keeping the Spoofs Out: Signal Authentication Services for Future GNSS. *Inside GNSS*, (nr 05-06), s. 48–55, 2011. [cytowanie na str. 23]

[80] O. Pozzobon, C. Wullems, K. Kubik. Secure Tracking using Trusted GNSS Receivers and Galileo Authentication Services. *Journal of Global Positioning Systems*, wol. 3 (nr 1-2), s. 200–207, 2004. [cytowanie na str. 22]

[81] M.L. Psiaki, B.W. O'Hanlon, J.A. Bhatti, D.P. Shepard, T.E. Humphreys. Gps spoofing detection via dual-receiver correlation of military signals. *Aerospace and Electronic Systems, IEEE Transactions on*, wol. 49 (nr 4), s. 2250–2267, 2013. [cytowanie na str. 22]

[82] M.L. Psiaki, S.P. Powell, B.W. O'Hanlon. GNSS Spoofing Detection, Correlating Carrier Phase with Rapid Antenna Motion. *GPS World*, (06), s. 53–58, 2012. [cytowanie na str. 21]

[83] Rohde & Schwarz. *R&S SMU200A Vector Signal Generator*. Specyfikacja techniczna: http://www.rohde-schwarz.com/en/product/smu200a-productstartpage_63493-7555.html. [cytowanie na str. 100]

[84] D. Sathyamoorthy. Global navigation satellite system (GNSS) spoofing: A review of growing risks and mitigation steps. *Defence S&T Technical Bulletin*, wol. 6 (nr 1), s. 42–61, 2013. [cytowanie na str. 18]

[85] L. Scott. What is adaptive nulling vs. adaptive beamforming? What are the advantaqes and disadvantages? *Inside GNSS*, (nr 04), s. 20–22, 2006. [cytowanie na str. 30]

[86] M.S. Sharawi, D.M. Akos, D.N. Aloi. GPS C/N0 estimation in the presence of interference and limited quantization levels. *Aerospace and Electronic Systems, IEEE Transactions on*, wol. 43 (nr 1), s. 227–238, 2007. [cytowanie na str. 49]

[87] D. Shepard. Characterization of receiver response to spoofing attacks. Praca magisterska, University of Texas, Austin, USA, 2011. [cytowanie na str. 13]

[88] D.P. Shepard, J.A. Bhatti, T.E. Humphreys. Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle. *GPS World*, wol. 23 (nr 8), s. 30–33, 2012. [cytowanie na str. 14, 23]

[89] D.P. Shepard, J.A. Bhatti, T.E. Humphreys. Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks. *International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, , s. 3591 – 3605, 2012. Nashville, USA. [cytowanie na str. 14]

[90] D.P. Shepard, T.E. Humphreys, A.A. Fansler. Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks. *International Journal of Critical Infrastructure Protection*, wol. 5 (nr 3–4), s. 146 – 153, 2012. [cytowanie na str. 14]

[91] Stanford Research Systems. *FS725 — Benchtop rubidium frequency standard*. Specyfikacja techniczna: http://www.thinksrs.com/downloads/PDFs/Catalog/FS725c.pdf. [cytowanie na str. 89]

[92] T.E. Tuncer, B. Friedlander. *Classical and Modern Direction-of-Arrival Estimation*. Academic Press, 2009. [cytowanie na str. 27]

[93] M. Uthansakul, M.E. Bialkowski. Wideband beam and null steering using a rectangular array of planar monopoles. *Microwave and Wireless Components Letters, IEEE*, wol. 16 (nr 3), s. 116–118, 2006. [cytowanie na str. 29]

[94] M. Uthansakul, P. Uthansakul. Null steering scheme for wideband spatial beamformer. *Microwave Conference, 2007. APMC 2007. Asia-Pacific*, , s. 1–4, Dec 2007. [cytowanie na str. 30]

[95] John A. Volpe National Transportation Systems Center. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. Final report, 2001. [cytowanie na str. 18]

[96] J.S. Warner, R. Johnston. GPS Spoofing Countermeasures. *Journal of Homeland Security*, 2003. http://lewisperdue.com/DieByWire/GPS-Vulnerability-LosAlamos.pdf. [cytowanie na str. 18]

[97] H. Wen, P. Huang, J. Dyer, A. Archinal, J. Fagan. Countermeasures for GPS Signal Spoofing. *18th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2005)*, , s. 1285–1290, 2005. [cytowanie na str. 19]

[98] K. Wesson, D. Shepard, T. Humphreys. Straight Talk on Anti-Spoofing: Securing the Future of PNT. *GPS World*, wol. 23 (nr 1), s. 32–34, 59–63, 2012. [cytowanie na str. 25]

[99] Y. Wu, S. Rhodes, E.H. Satorius. Direction of arrival estimation via extended phase interferometry. *Aerospace and Electronic Systems, IEEE Transactions on*, wol. 31 (nr 1), s. 375–381, 1995. [cytowanie na str. 28]

[100] C.J. Wullems. A Spoofing Detection Method for Civilian L1 GPS and the E1-B Galileo Safety of Life Service. *Aerospace and Electronic Systems, IEEE Transactions on*, wol. 48 (nr 4), s. 2849–2864, 2012. [cytowanie na str. 22]

[101] P. Zalewski. Real-time GNSS spoofing detection in maritime code receivers. *Zeszyty Naukowe/Akademia Morska w Szczecinie*, wol. 38 (nr 110), s. 118–124, 2014. [cytowanie na str. 23]

[102] N.I. Ziedan. *GNSS Receivers for Weak Signals*. Artech House Space Technology and Applications. Artech House, 2006. [cytowanie na str. 10]

[103] M.D. Zoltowski, A.S. Gecan. Advanced adaptive null steering concepts for GPS. *Military Communications Conference, 1995. MILCOM '95, Conference Record, IEEE*, wol. 3, , s. 1214–1218, 1995. [cytowanie na str. 30]

Spis symboli i skrótów

Symbol	Opis
θ	Kąt elewacji kierunku nadejścia sygnału
ρ_i	Pseudoodległość od i-tego satelity
$\delta\phi$	Korekta fazy początkowej fali nośnej w segmencie sygnału
$\epsilon_{\Delta\phi}$	Błąd średni estymacji opóźnień fazowych
$\sigma_{\Delta\phi}$	Odchylenie standardowe błędu estymacji opóźnień fazowych
ϕ	Faza początkowa fali nośnej
ψ	Kąt azymutu kierunku nadejścia sygnału
τ_n	Względne przesunięcie czasowe dwóch sygnałów, wyrażone w próbkach
Γ	Funkcja celowa do optymalizacji wektora wagowego
$\Delta\phi_{i,j}\|s_k$	Opóźnienie fazy sygnału k-tego satelity pomiędzy i-tym i j-tym elementem antenowym
Δf_D	Poprawka odchyłki dopplerowskiej
$\Phi_{i,j\|s_k,s_l}$	Różnica opóźnień fazowych pomiędzy i-tym a j-tym elementem antenowym, obliczona dla sygnałów satelitów s_k i s_l
Φ_{prog}	Wartość progowa różnicy opóźnień fazowych w detekcji spoofingu
c	Prędkość światła w próżni
$d_{i,j}$	Odległość pomiędzy i-tym i j-tym elementem szyku antenowego
f_D	Dokładna odchyłka dopplerowska fali nośnej

Symbol	Opis
$f_{D,zgr}$	Odchyłka dopplerowska fali nośnej oszacowana zgrubnie
f_n	Częstotliwość nośna sygnału GPS
r_{xy}	Funkcja korelacji skrośnej dwóch sygnałów
$\mathbf{s}$	Wektor próbek z wyjśc elementów szyku antenowego
s_{fp}	Sygnał na wyjściu bloku filtracji przestrzennej
s_{nad}	Sygnał GPS nadawany przez satelitę
$s_{odb,m}$	Sygnał GPS odbierany na wejściu m-tego elementu szyku antenowego
t_n	Numer próbki sygnału
t_u	Różnica taktów zegarów odbiornika i satelity
$\mathbf{w}$	Wektor wag szyku antenowego
x_u, y_u, z_u	Współrzędne położenia odbiornika
$x_{sat,n}$, $y_{sat,n}$, $z_{sat,n}$	Współrzędne położenia n-tego satelity
$C_{C/A}$	Sekwencja pseudolosowa Coarse/Acquisition
$\frac{C}{N_0}$	Stosunek mocy fali nośnej do widmowej gęstości mocy szumu
$\overline{\frac{C}{N_0}}_{\in S_{spoof}}$	Średnia wartość $\frac{C}{N_0}$ sygnałów fałszywych przed filtracją przestrzenną
$\overline{\frac{C}{N_0}}_{\in S_{spoof}\ filtr}$	Średnia wartość $\frac{C}{N_0}$ sygnałów fałszywych po filtracji przestrzennej
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}}$	Średnia wartość $\frac{C}{N_0}$ sygnałów prawdziwych przed filtracją przestrzenną
$\overline{\frac{C}{N_0}}_{\notin S_{spoof}\ filtr}$	Średnia wartość $\frac{C}{N_0}$ sygnałów prawdziwych po filtracji przestrzennej
D	Sekwencja danych depeszy nawigacyjnej GPS
G	Charakterystyka odbiorcza szyku antenowego dla sygnału harmonicznego
G_{GPS}	Charakterystyka odbiorcza szyku antenowego dla szerokopasmowego sygnału GPS C/A
G_{szum}	Zmiana mocy szumu pomiędzy wejściem a wyjściem filtru przestrzennego
N_{det}	Całkowita liczba detekcji spoofingu w serii pomiarowej
$N_{det\ OK}$	Liczba detekcji spoofingu z poprawnym określeniem numerów fałszywych sygnałów

Symbol	Opis
$N_{det\ \subset S_{spoof}}$	Liczba detekcji spoofingu z niewykryciem jednego lub więcej fałszywych sygnałów
$N_{det\ \notin S_{spoof}}$	Liczba detekcji spoofingu z uznaniem co najmniej jednego sygnału prawdziwego za fałszywy
$N_{det\ \subset S_{spoof}, \notin S_{spoof}}$	Liczba detekcji spoofingu z niewykryciem jednego lub więcej fałszywych sygnałów i uznaniem co najmniej jednego sygnału prawdziwego za fałszywy
N_{sat}	Liczba widocznych satelitów
P_D	Prawdopodobieństwo detekcji
P_{FA}	Prawdopodobieństwo fałszywego alarmu
P_i	Moc sygnału na wejściu i-tego elementu szyku antenowego
P_{nad}	Moc sygnału nadawanego
$P_{sygn\ [\sim det \mid \in S_{spoof}]}$	Rozkład liczby niewykrytych sygnałów fałszywych
$P_{sygn\ [\in S_{spoof} \mid \notin S_{spoof}]}$	Rozkład liczby prawdziwych sygnałów uznanych za fałszywe
$P_{\notin S_{spoof}}$	Rozkład liczby sygnałów prawdziwych przed filtracją przestrzenną
$P_{\notin S_{spoof}\ filtr}$	Rozkład liczby sygnałów prawdziwych po filtracji przestrzennej
S_{odb}	Zbiór wszystkich odbieranych w danej chwili sygnałów GPS
S_{spoof}	Zbiór sygnałów nadawanych przez spoofer
$T_{n,1ms}$	Liczba próbek sygnału w czasie trwania 1 ms
$X[k]$	k-ty prążek widma sygnału dyskretnego x$[t_n]$

Skrót	Rozwinięcie
ADC	Analog-to-Digital Converter
ARW	Automatyczna Regulacja Wzmocnienia (ang. AGC - Automatic Gain Control)
C/A	Coarse Acquisition
CDMA	Code Division Multiple Access
DoA	Direction of Arrival

Skrót	Rozwinięcie
DS-CDMA	Direct Sequence CDMA
DSSS	Direct Sequence Spread Spectrum
FDMA	Frequency Division Multiple Access
FPGA	Field Programmable Gate Array
GUI	Graphical User Interface
GPS	Global Positionig System
GNSS	Global Navigation Satellite System
LoS	Line od Sight
MEO	Medium Earth Orbit
MMSE	Minimum Mean Square Error
MUSIC	MUltiple SIgnal Classification
NLoS	Non Line of Sight
PRN	Pseudo Random Noise
PDOP	Position Dilution of Precision
PI	Power Inversion
PPS (1)	Precise Positioning Service
PPS (2)	Pulse-per-second
PSO	Particle Swarm Optimization
PVT	Position, Velocity and Time
RAIM	Receiver Autonomous Integrity Monitoring
SDR	Software Defined Radio
SNR	Signal-to-Noise Ratio
SPS	Standard Positioning Service
ToA	Time of Arrival
UAV	Unmanned Aerial Vehicle
USRP	Universal Software Radio Peripheral
VSD	Vestigial Signal Detection

Spis rysunków

Spis tabel