System wykrywania i przeciwdziałania zakłóceniom celowym odbiornika GPS

Dr inż. Jarosław Magiera, prof. dr hab. inż. Ryszard J. Katulski
Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki

Współcześnie nawigacja morska jest realizowana przede wszystkim w oparciu o informacje pozyskiwane za pośrednictwem odbiorników globalnych systemów nawigacji satelitarnej – GNSS. Do grupy tych systemów, wykazujących pełną gotowość operacyjną, zaliczają się amerykański GPS i rosyjski GLONASS, a także satelitarne geostacjonarne systemy wspomagające jak WAAS (USA) czy EGNOS (Europa). Niezaprzeczalnymi zaletami systemów GNSS są ich globalny zasięg, stosunkowo duża dokładność wyznaczanej pozycji, brak opłat za korzystanie oraz szeroki wybór dostępnych na rynku odbiorników. Należy jednak mieć na uwadze to, że ograniczanie się do jednego źródła danych nawigacyjnych wiąże się z ryzykiem. Istnieje bowiem szereg sytuacji, w których skorzystanie z informacji dostarczanych przez satelity GPS czy GLONASS może być utrudnione lub wręcz niemożliwe. W przypadku żeglugi realizowanej w niewielkich odległościach od linii brzegowej dobrym wsparciem dla nawigacji satelitarnej może być nawigacja terestryczna lub radarowa. W przypadku żeglugi pełnomorskiej i oceanicznej jest możliwe jedynie wspomaganie GNSS nawigacją zliczeniową lub inercyjną, które jednakże wyznaczają położenie względem jednej z poprzednich pozycji statku oraz są obarczone narastającym błędem dokładności. Alternatywą jest nawigacja astronomiczna, która wymaga odpowiednich umiejętności nawigatora oraz korzystnych warunków meteorologicznych.

Działanie systemów GNSS, w tym zapewnienie możliwości powszechnego dostępu do sygnałów nawigacyjnych, jest regulowane przez rządy państw, do których należą satelity i naziemna infrastruktura kontrolna poszczególnych systemów. Nie jest zatem wykluczone, że, w szczególnych warunkach, korzystanie z takiego systemu będzie ograniczone na przykład do armii danego kraju. Taki scenariusz jest jednak znacznie mniej prawdopodobny niż sytuacja, w której poprawny odbiór sygnałów z satelitów jest niemożliwy ze względu na, nieświadome lub celowe, zakłócanie tych sygnałów. Należy mieć świadomość tego, że sygnały pochodzące z satelitów GNSS mają przy powierzchni Ziemi moc rzędu 10^{-16} W [4], czyli wielokrotnie mniejszą od mocy szumu termicznego o takiej samej szerokości pasma częstotliwości. Zatem, nawet urządzenie nadające sygnały o stosunkowo niewielkiej mocy (rzędu kliku watów) może uniemożliwić funkcjonowanie odbiorników GNSS w promieniu wielu kilometrów. Aktualnie w sprzedaży są oferowane przenośne lub samochodowe urządzenia zagłuszające sygnały GPS (ang. *GPS jammers*), pomimo że ich użytkowanie jest niezgodne z prawem [6]. Zagłuszanie jest najprostszą formą zakłócania, w której szerokopasmowy sygnał niepożądany ma zwykle charakter pseudoszumowy lub postać fali ciągłej z liniową modulacją częstotliwości.

Znacznie bardziej zaawansowaną formą zaburzania pracy odbiorników GNSS jest tzw. spoofing. W tym przypadku urządzenie zakłócające (spoofer) emituje sygnały imitujące te, które docierają z satelitów nawigacyjnych do odbiornika stanowiącego cel ataku. Parametry sygnałów imitujących oraz depesze w nich zawarte są dobrane tak, aby na ich podstawie odbiornik wyznaczył nieprawidłowe wartości bieżącego położenia, prędkości lub czasu. W przeciwieństwie do zagłuszania, moc sygnałów niepożądanych na wejściu odbiornika nie musi być wielokrotnie większa od mocy sygnałów odbieranych z satelitów [2].

Prowadzone na całym świecie niezależne badania wykazały, że cywilne odbiorniki systemu GPS, korzystające wyłącznie z sygnałów C/A nadawanych w pasmie L1, są podatne na ataki typu spoofing. Próby przeprowadzane w kontrolowanych warunkach wykazały możliwość zdalnej modyfikacji współrzędnych położenia wyznaczanych przez odbiorniki [8]. Zagrożenie dla nawigacji morskiej potwierdza eksperyment przeprowadzony latem 2013 roku przez zespół z Texas University. Poprzez spoofing GPS zdołali oni spowodować zmianę kursu luksusowego jachtu płynącego po Morzu Śródziemnym [1]. Jest to przykład obrazujący potencjał zagrożenia dla wszystkich pojazdów sterowanych w sposób autonomiczny na podstawie sygnałów nawigacji satelitarnej.

Ze względu na określoną postać i stosunkowo niewielką moc sygnałów imitujących, a także ze względu na brak jednoznacz-

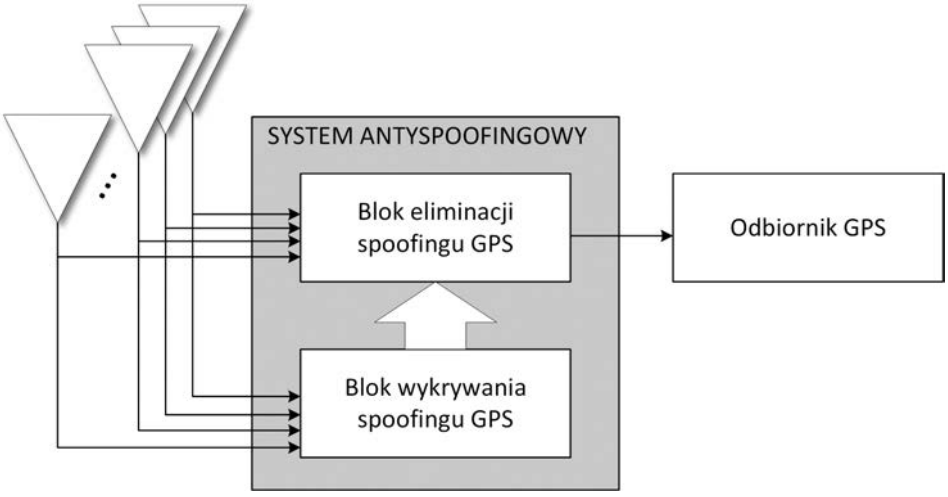
nych objawów nieprawidłowej pracy odbiornika, wykrycie spoofingu konwencjonalnymi metodami (na przykład analiza widmowa) jest praktycznie niemożliwe. Pomimo, że na rynku są dostępne odbiorniki GPS wyposażone w środki ochrony przed zagłuszaniem [9], dotychczas nie są oferowane urządzenia, które zapewniałyby skuteczną ochronę przed spoofingiem. W związku z tym, zachodzi potrzeba opracowania efektywnych rozwiązań antyspoofingowych.

W publikacjach naukowych poświęconych problemowi spoofingu GNSS można znaleźć propozycje sposobów przeciwdziałania skutkom takiego ataku [7]. Zasadniczo, można wyróżnić dwie grupy metod antyspoofingowych. Do pierwszej z nich należą metody związane z samym wykryciem obecności spoofingu. Z kolei druga grupa obejmuje rozwiązania umożliwiające zapewnienie prawidłowej pracy odbiornika, do którego docierają sygnały imitujące. Metody w ramach każdej z tych grup są w dużym stopniu zróżnicowane pod względem niezawodności, a także złożoności implementacyjnej i nakładu przetwarzania. Najprostsze metody wymagają jedynie modyfikacji oprogramowania odbiornika, jednakże zwykle są one skuteczne jedynie w przypadku mniej wyrafinowanych ataków, w których parametry sygnałów imitujących (na przykład moc czy stosunek sygnał – szum) znacząco odbiegają od wartości obserwowanych w przypadku odbioru autentycznych sygnałów. Skuteczną ochronę przeciwko spoofingowi mogłoby zapewnić wprowadzenie weryfikacji autentyczności odbieranych sygnałów poprzez środki kryptograficzne. Takie rozwiązanie wymaga jednakże modyfikacji po stronie satelitów, a ponadto musiałoby ono zapewniać kompatybilność z dotychczasowymi odbiornikami. Inną skuteczną metodą zabezpieczenia przed spoofingiem jest korzystanie z dodatkowego niezależnego źródła informacji o czasie i położeniu, niemniej zastosowanie takiego rozwiązania nie zawsze jest możliwe. Biorąc pod uwagę jedynie metody antyspoofingowe niewymagające modyfikacji istniejących sygnałów oraz korzystania z innych systemów, za najbardziej niezawodne można uznać te, które bazują na analizie przestrzenno-czasowej odbieranych sygnałów GNSS [3]. Zakłada się w nich, że wszystkie sygnały imitujące są nadawane przez spoofer za poprzez tę samą antenę i, w związku z tym, docierają do odbiornika z tego samego kierunku. W niniejszej publikacji zaprezentowano autorską koncepcję systemu antyspoofingowego działającego właśnie na podstawie metod przestrzennej analizy i przetwarzania sygnałów GPS. W kolejnej części referatu opisano główne założenia dotyczące zasady działania i budowy systemu. Następnie, przedstawiono implementację prototypu tego systemu służącego do empirycznej weryfikacji efektywności wykrywania i eliminacji spoofingu. W ostatniej części dokonano analizy wybranych wyników przeprowadzonych badań pomiarowych.

SYSTEM ANTYSPOOFINGOWY GPS

Jak wspomniano, metody wykrywania spoofingu GNSS poprzez analizę parametrów przestrzennych były już opisywane w literaturze. Niemniej jednak, dotychczas nie zaproponowano kompleksowego rozwiązania, które umożliwiałoby zarówno detekcję, jak również eliminację sygnałów imitujących na wejściu odbiornika. W opisywanym systemie, którego schemat przedstawiono na rys. 1, detekcja spoofingu bazuje na analizie sygnałów GPS odbieranych przez M elementów szyku antenowego. Wartości parametrów wyznaczane podczas tej analizy są przekazywane do modułu eliminacji spoofingu, który dokonuje selektywnej filtracji sygnałów imitujących, charakteryzujących się takimi samymi właściwościami kierunkowymi. Dominującymi składowymi sygnału na wyjściu systemu są sygnały autentyczne pochodzące z satelitów. Taki sygnał, podany na wejście standardowego odbiornika GPS, powinien umożliwiać estymację prawidłowych danych o czasie, położeniu i prędkości odbiornika.

Aby odbiornik GPS mógł określić swoje położenie w trójwymiarowym układzie współrzędnych, konieczny jest odbiór sygnałów pochodzących z co najmniej czterech satelitów. Zatem spoofer, imitujący rzeczywistą konstelację satelitów, nadaje nie mniej niż cztery sygnały GPS równocześnie. W takim przypadku spoofing można wykryć, stwierdzając odbiór co najmniej czterech sygnałów pochodzących z tego samego kierunku, co w przypadku braku spoofingu jest sytuacją niespotykaną. W proponowanym rozwiązaniu nie jest dokonywana estymacja samych kierunków nadejścia sygnałów, gdyż błąd estymacji tego parametru jest zależny od liczby i ułożenia anten w szyku oraz od rzeczywistego kierunku nadejścia sygnału. Ponadto, wyznaczenie właściwego kierunku nadejścia sygnału wymaga



Rys. 1. Schemat systemu ochrony przed spoofingiem GPS

precyzyjnej kalibracji szyku antenowego. Zamiast tego, dla każdego odbieranego sygnału są estymowane jego opóźnienia fazowe wynikające z różnic czasu propagacji od źródła do poszczególnych elementów antenowych szyku. Dzięki temu prawdopodobieństwo detekcji spoofingu, które zależy od błędu estymacji tych opóźnień, nie jest uzależnione od kierunku nadejścia sygnałów imitujących do odbiornika.

Właściwy proces detekcji spoofingu polega na porównaniu odpowiednich opóźnień fazowych wyznaczonych dla wszystkich sygnałów GPS odbieranych w danej chwili. Jeśli wśród tych sygnałów znajdują się takie, dla których wszystkie różnice opóźnień fazowych są mniejsze niż pewna wartość progowa, zostaje podjęta pozytywna decyzja o wykryciu spoofingu. Wartość progu detekcji jest uzależniona od czynników takich jak: dopuszczalne prawdopodobieństwo fałszywego alarmu, jakość odbieranych sygnałów imitujących (wyrażona stosunkiem sygnał – szum) oraz hipotetyczna liczba tych sygnałów. Wszystkie sygnały, dla których będą stwierdzone odpowiednio małe różnice opóźnień fazowych, zostają uznane za sygnały imitujące.

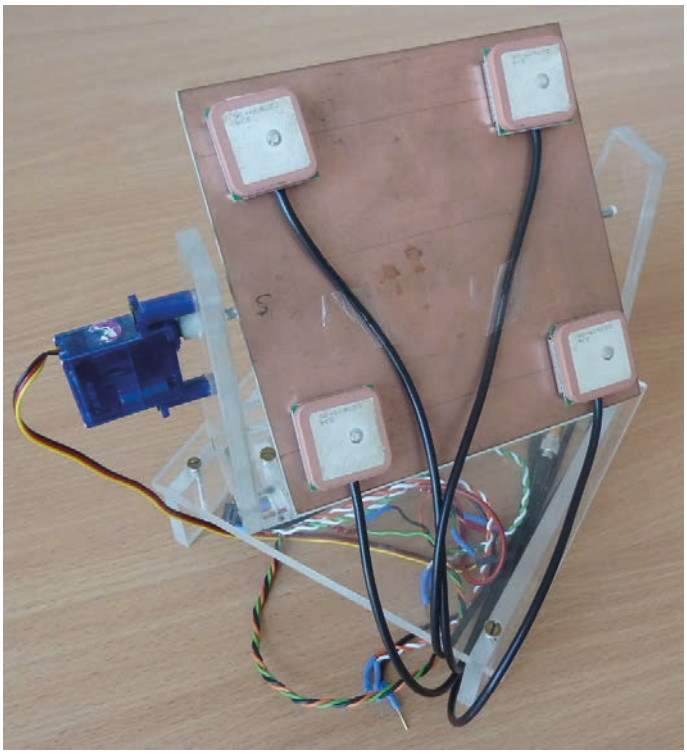
Blok eliminacji sygnałów imitujących, podobnie jak moduł detekcji spoofingu, przetwarza sygnały z wyjść wszystkich elementów szyku antenowego. Proces eliminacji jest realizowany poprzez adaptacyjną filtrację przestrzenną. Polega ona na takim ukształtowaniu charakterystyki odbiorczej szyku antenowego, aby sygnały docierające z określonego kierunku (sygnały charakteryzujące się takimi samymi wartościami opóźnień fazowych) były tłumione znacznie silniej niż sygnały z innych kierunków. Taki sposób formowania charakterystyki kierunkowej jest nazywany kierowaniem zerami (ang. *null-steering*). Uzyskanie pożądanego kształtu jest możliwe poprzez fazowanie szyku, czyli odpowiednią modyfikację zależności fazowych (często również amplitudowych) pomiędzy sygnałami z wyjść poszczególnych anten odbiorczych. W zaproponowanym systemie fazowanie szyku jest realizowane w oparciu o, wyznaczone na etapie detekcji spoofingu, uśrednione wartości opóźnień fazowych sygnałów imitujących. Zatem realizowana filtracja przestrzenna ma charakter adaptacyjny, uzależniony od aktualnego kierunku nadejścia sygnałów spoofera. Na możliwy do uzyskania poziom tłumienia tych sygnałów ma wpływ dokładność estymacji opóźnień fazowych, uzależniona od stosunku sygnał – szum.

Wstępną ocenę efektywności prezentowanego systemu przeprowadzono na drodze badań symulacyjnych. W ramach tych badań dokonano oszacowania prawdopodobieństwa detekcji spoofingu dla przypadków odbioru od czterech do ośmiu sygnałów imitujących o rożnych wartościach stosunku sygnał – szum. Stwierdzono, że, dla dopuszczalnego prawdopodobieństwa fałszywego alarmu na poziomie 10^{-4}, wysokie prawdopodobieństwo detekcji można uzyskać już dla czterech sygnałów imitujących o przeciętnej jakości (parametr C/N_0 powyżej 40 dBHz). Natomiast przy większej liczbie sygnałów imitujących prawidłowa detekcja spoofingu jest możliwa również dla sygnałów o gorszej jakości. Poprzez symulacje wykazano również, że proces filtracji przestrzennej, w warunkach pełnej widoczności nieba, nie będzie eliminował sygnałów autentycznych w stopniu uniemożliwiającym wyznaczenie pozycji odbiornika. Bardziej szczegółowy opis oraz wyniki przeprowadzonych badań symulacyjnych można znaleźć w [5].

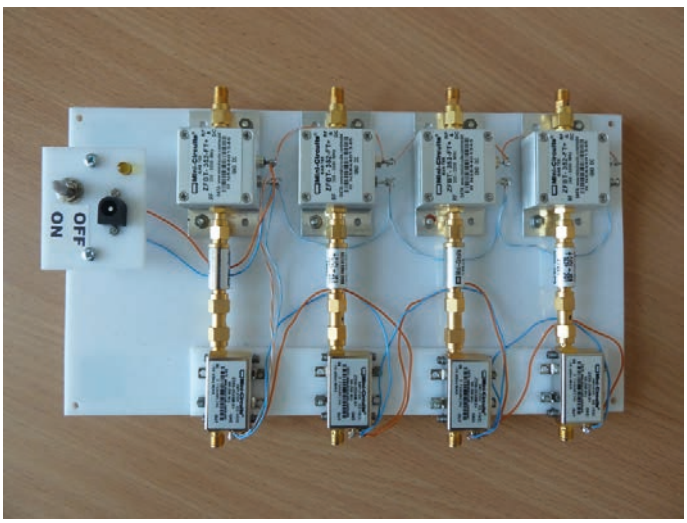
PROTOTYP SYSTEMU

Badania symulacyjne umożliwiły uzyskanie pozytywnej odpowiedzi na pytanie o zasadność stosowania proponowanego rozwiązania w celu wykrywania i eliminacji spoofingu GPS. Jednakże, aby dokonać pełnej oceny efektywności systemu, konieczna była realizacja badań pomiarowych w warunkach laboratoryjnych i polowych. Do przeprowadzenia takich badań niezbędny był prototyp systemu.

Prototyp opracowano w technice radia programowalnego SDR (ang. *software defined radio*), co oznacza, że jego działanie jest w głównej mierze oparte na algorytmach cyfrowego prze-



Rys. 2. Czteroelementowy szyk aktywnych anten GPS



Rys. 3. Analogowe tory sygnałowe w.cz.

twarzania sygnałów realizowane przez oprogramowanie. Sprzętowa, analogowa część prototypu służy jedynie do wstępnego przetworzenia sygnałów. W jej skład wchodzi czteroelementowy szyk antenowy, którego widok przedstawiono na rys. 2. Zastosowano w nim aktywne anteny mikropaskowe o wzmocnieniu 24 dB. Tworzą one układ w konfiguracji kwadratu o boku długości 8,6 cm, co odpowiada 0,45 długości fali sygnału GPS na częstotliwości L1 równej 1575,42 MHz. Taka konfiguracja anten jest zgodna z modelem przyjętym w badaniach symulacyjnych.

Sygnały z wyjść anten są następnie przetwarzane w czterech identycznych torach w.cz. (rys. 3), na które składają się: układ zasilania anteny aktywnej (ang. *bias tee*), filtr pasmowoprzepustowy obejmujący pasmo L1 od 1530 MHz do 1620 MHz oraz wzmacniacz szerokopasmowy o wzmocnieniu około 39 dB. Funkcją torów w.cz. jest przede wszystkim zapewnienie odbieranym sygnałom GPS mocy wymaganej do poprawnej konwersji na postać cyfrową, która jest realizowana przez moduły radia programowalnego NI-USRP 2920. Przed właściwym przetworzeniem analogowo-cyfrowym moduły te sprowadzają sygnały z pasma w.cz. do pasma podstawowego i dokonują dolnoprzepustowej filtracji antyaliasingowej. Próbki z wyjścia przetwornika A/C są przesyłane, za pośrednictwem interfejsu Gigabit Ethernet, do komputera PC, którego oprogramowanie realizuje zasadniczą część przetwarzania sygnałów. Do poprawnej estymacji opóźnień fazowych sygnałów jest wymagana synchronizacja czasowa i częstotliwościowa modułów USRP. W prezentowanym prototypie jest ona zapewniana przez wzorzec rubidowy. Zestaw użytych czterech urządzeń USRP wraz z wzorcem częstotliwości przedstawiono na rys. 4.

Oprogramowanie komputera PC operuje na sekwencjach próbek sygnałów odbieranych przez wszystkie anteny szyku. Przetwarzanie sygnałów z pierwszej anteny różni się od pozostałych i rozpoczyna się od dwóch etapów, które są realizowane w każdym odbiorniku GPS. Pierwszym z tych etapów przetwarzania jest tak zwana akwizycja sygnałów GPS. Wynikiem tej procedury jest identyfikacja numerów satelitów przypisanych do odbieranych sygnałów (tak zwany SVID) oraz uzyskanie wstępnej synchronizacji czasowej i częstotliwościowej odbiornika do tych sygnałów. Po zakończeniu akwizycji każdy wykryty sygnał GPS podlega tak zwanemu procesowi śledzenia, w którym synchronizacja jest utrzymywana na bieżąco dzięki monitorowaniu, w dwóch sprzężonych ze sobą pętlach, zmian opóźnienia i częstotliwości sygnału. Podczas śledzenia jest odtwarzana replika odbieranego sygnału GPS. Mnożenie zespolone tej repliki z odpowiednimi sygnałami odbieranymi przez inne anteny umożliwia estymację opóźnień fazowych sygnału pomiędzy anteną pierwszą i pozostałymi. Następnie, wyznaczane są różnice odpowiednich opóźnień fazowych pomiędzy wszystkimi aktualnie odbieranymi sygnałami. Jeśli dla co najmniej czterech spośród tych sygnałów wszystkie różnice są mniejsze niż wartość progowa, zostaje stwierdzona obecność spoofingu. Próg detekcji jest uzależniony od rozpatrywanej liczby sygnałów odbieranych oraz od ich stosunku sygnał – szum.

W przypadku wykrycia spoofingu są wyznaczane uśrednione opóźnienia fazowe sygnałów imitujących. Opóźnienia te są przekazywane do modułu programowego realizującego funkcje filtru przestrzennego. Na podstawie bieżących wartości opóźnień są wyznaczane zespolone współczynniki wagowe, przez które są mnożone próbki sygnałów z poszczególnych anten. Suma sygnałów przemnożonych przez współczynniki odpowiada sygnałowi odbieranemu przez pojedynczą antenę o charakterystyce kierunkowej wykazującej silne tłumienie sygnałów nadchodzących z jednego ustalonego kierunku. Modyfikacja współczynników umożliwia adaptacyjny wybór tego kierunku.

POMIAROWE BADANIA EFEKTYWNOŚCI SYSTEMU

Badania z użyciem opracowanego prototypu przeprowadzono w trzech etapach. Różniły się one warunkami transmisji sygnałów oraz konfiguracją stanowiska badawczego. We wszystkich badaniach rolę spoofera, czyli źródła sygnałów imitujących, pełnił wektorowy generator sygnałów umożliwiający nadawanie maksymalnie ośmiu sygnałów GPS równocześnie.

Celem badań realizowanych w pierwszym etapie była weryfikacja wyników badań symulacyjnych, w których określono prawdopodobieństwo detekcji spoofingu w funkcji stosunku sygnał – szum (parametr C/N_0) oraz liczby sygnałów imitujących. Prawdopodobieństwo detekcji w badaniach pomiarowych stanowiło procent czasu, w którym wszystkie różnice opóźnień fazowych dla określonej liczby odbieranych sygnałów były mniejsze

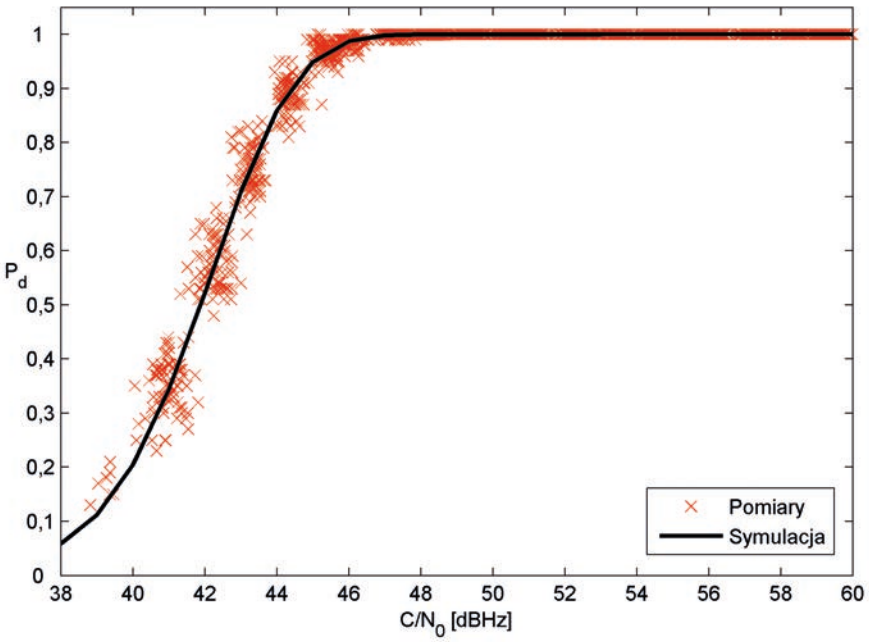
Rys. 4. Moduły radia programowalnego oraz rubidowy wzorzec częstotliwości

niż wartość progowa. Aby zapewnić warunki transmisji zbliżone do modelu kanału przyjętego w badaniach symulacyjnych (kanał z addytywnym białym szumem gaussowskim), generator sygnałów połączono przewodowo z wejściami torów w.cz. prototypu systemu. Wyniki uzyskane dla przypadku transmisji czterech sygnałów imitujących przedstawiono na rys. 5. Analizowany zakres zmienności parametru C/N_0 obejmował wartości od 38 dBHz (sygnały o niskiej jakości) do 63 dBHz (sygnały o bardzo wysokiej jakości). Czarna krzywa reprezentuje zależność prawdopodobieństwa detekcji spoofingu od C/N_0, uzyskaną poprzez aproksymację wyników badań symulacyjnych. Jak można zauważyć, wyniki badań pomiarowych są zbieżne z tą krzywą. Zgodność wyników symulacji i pomiarów stwierdzono również dla scenariuszy, w których nadawano od pięciu do ośmiu sygnałów GPS.

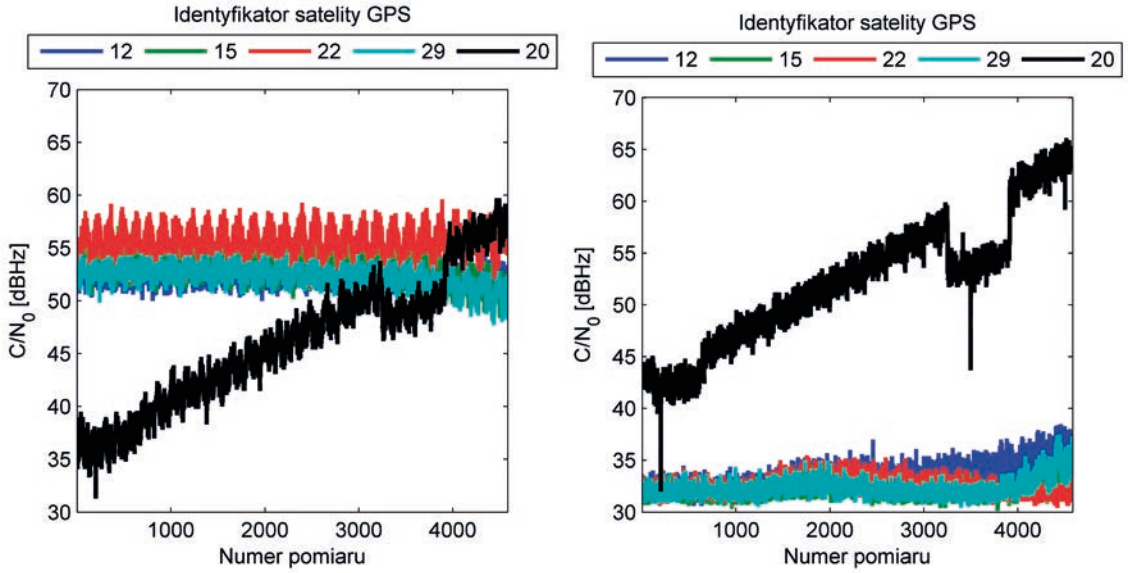
Badania przeprowadzone w drugim etapie służyły wykazaniu poprawności działania algorytmu filtracji przestrzennej w warunkach laboratoryjnych. Wymagało to zestawienia stanowiska badawczego w taki sposób, aby na wejściach prototypu były obecne sygnały o różnych opóźnieniach fazowych. W tej konfiguracji generator wytwarzał pięć sygnałów GPS. Cztery z nich, odpowiadające sygnałom imitującym o identyfikatorach SVID 12, 15, 22 i 29, były przesyłane przewodowo, podobnie jak w etapie pierwszym. Natomiast piąty sygnał, reprezentujący sygnał rzeczywisty o identyfikatorze 20, był nadawany drogą radiową i odbierany przy użyciu szyku antenowego. Był on sumowany z sygnałami imitującymi przed podaniem na wejście torów w.cz. prototypu. Oceny działania filtru przestrzennego dokonano poprzez obserwację wartości parametru C/N_0 poszczególnych sygnałów przed i po filtracji. Na rys. 6. przedstawiono uzyskane wyniki. Po lewej stronie zobrazowano wartości C/N_0 zarejestrowane dla przypadku bez użycia filtracji przestrzennej. Dla sygnałów imitujących, nadawanych ze stałą mocą, wartość C/N_0 utrzymywała się na wysokim poziomie powyżej 50 dBHz. Natomiast moc sygnału o identyfikatorze 20 była stopniowo zwiększana w trakcie badania, począwszy od poziomu odpowiadającego wartości C/N_0 około 35 dBHz do osiągnięcia wartości C/N_0 zbliżonej do sygnałów imitujących. Wykres po prawej stronie przedstawia wartości C/N_0 dla tych samych sygnałów, w tych samych chwilach, jednakże z zastosowaniem filtracji przestrzennej. Jest zauważalny wyraźny spadek wartości C/N_0 sygnałów imitujących poniżej 35 dBHz, co odpowiada stosunkowi mocy sygnał – szum mniejszemu od -28 dB, a więc sygnałowi o bardzo niskiej jakości. Widoczna jest poprawa jakości sygnału rzeczywistego, dla którego średni wzrost C/N_0, wywołany stłumieniem sygnałów imitujących, wyniósł około 7 dB. Można na tej podstawie stwierdzić, że implementację algorytmu filtracji przestrzennej wykonano poprawnie.

W ostatnim etapie badań przeprowadzono testy systemu w warunkach polowych, co umożliwiło dokonanie jego oceny z punktu widzenia praktycznego zastosowania. W tym etapie szyk antenowy znajdował się na zewnątrz budynku i docierały do niego rzeczywiste sygnały z satelitów GPS oraz sygnały imitujące nadawane przez generator połączony z anteną kierunkową umieszczoną wewnątrz budynku. Aby określić warunki referencyjne dla oceny działania systemu, w pierwszej kolejności dokonano analizy liczności i wartości C/N_0 sygnałów rzeczywistych odbieranych przy braku spoofingu. Najczęściej odbierano sygnały z trzech lub czterech satelitów (odpowiednio 40% i 33% pomiarów). Ta stosunkowo niewielka liczba sygnałów była spowodowana przesłonięciem części nieba przez budynek. Z kolei najczęściej rejestrowana wartość C/N_0 była równa 42 dBHz.

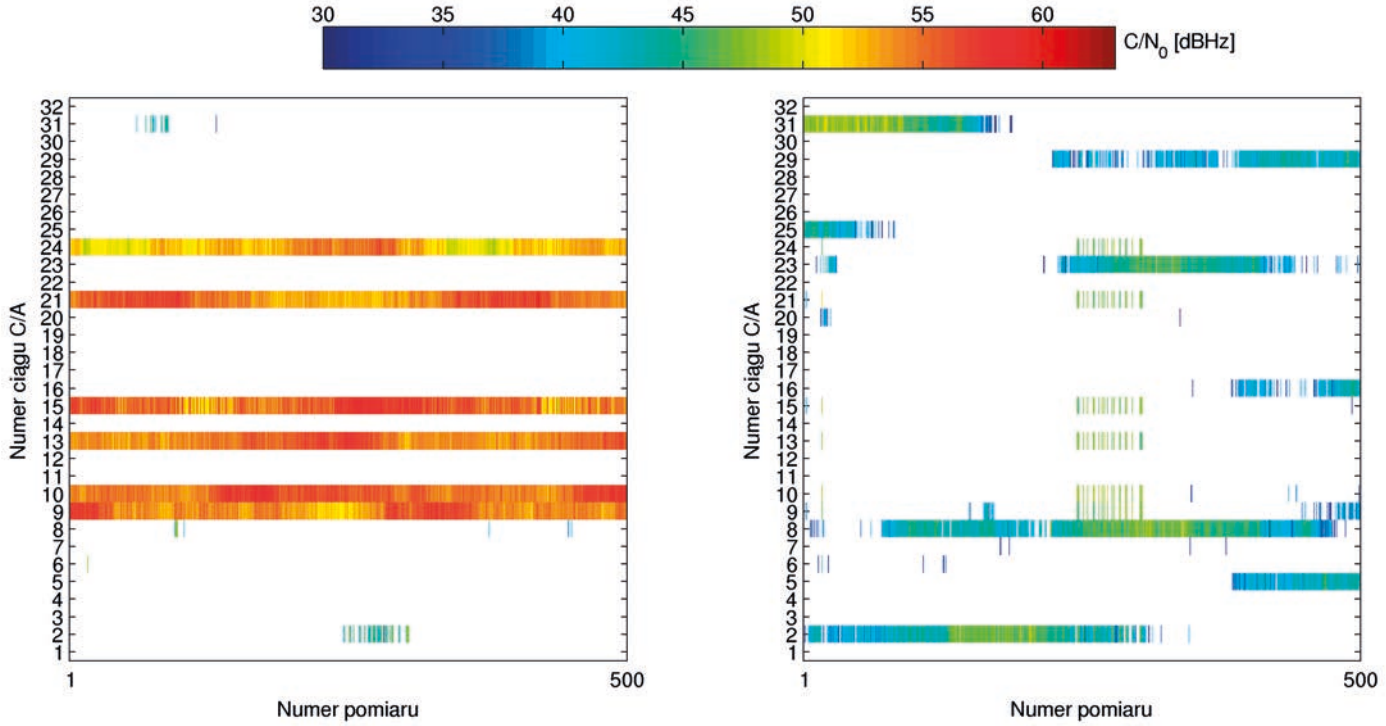
We właściwych badaniach, prowadzonych w obecności spoofingu, generator, podobnie jak w etapie pierwszym, nadawał od czterech do ośmiu sygnałów GPS. W celu dokonania oceny efektywności systemu analizowano liczbę sygnałów rzeczywistych oraz wartości C/N_0 wszystkich odbieranych sygnałów GPS przed i po filtracji przestrzennej. Na rys. 7 zobrazowano wartości C/N_0 zarejestrowane w przypadku scenariusza, w którym nadawano sześć sygnałów imitujących. Na każdym z wykresów oś pozioma reprezentuje numer pomiaru, oś pionowa identyfikator satelity SVID. Skala kolorów odpowiadających



Rys. 5. Wyniki pomiarów prawdopodobieństwa detekcji spoofingu w obecności czterech sygnałów imitujących



Rys. 6. Wartości C/N_0 przed i po filtracji przestrzennej (warunki laboratoryjne)



Rys. 7. Wartości C/N_0 przed i po filtracji przestrzennej (warunki rzeczywiste)

zmierzonym wartościom C/N_0 obejmuje zakres od 30 dBHz (kolor niebieski) do 63 dBHz (kolor czerwony). Wykres po lewej stronie reprezentuje warunki przed filtracją przestrzenną, gdzie było obecnych sześć sygnałów imitujących (SVID: 9, 10, 13, 15, 21 i 24) o wartościach C/N_0 powyżej 50 dBHz. Obecność pojedynczych sygnałów rzeczywistych stwierdzano w stosunkowo niewielkiej liczbie pomiarów, gdyż zostały one zamaskowane przez sygnały spoofera.

Na wykresie po prawej stronie, reprezentującym sytuację po eliminacji spoofingu, widać, że sygnały imitujące wyeliminowano całkowicie oraz, że znacząco poprawiła się możliwość odbioru sygnałów rzeczywistych. Średnia wartość C/N_0 sygnałów imitujących zmalała z 54,4 dBHz do 37,9 dBHz, natomiast w przypadku sygnałów autentycznych wzrosła z 32,3 dBHz do 43,2 dBHz. Dane dotyczące rozkładu liczby odbieranych sygnałów rzeczywistych przedstawiono w tabl. 1. Przed eliminacją spoofingu w niemal 90% pomiarów nie był możliwy odbiór ani jednego sygnału z satelity GPS. Natomiast po zastosowaniu filtracji przestrzennej w ponad 80% przypadków wykrywano co najmniej trzy sygnały rzeczywiste. Najczęściej był możliwy odbiór dokładnie trzech sygnałów, co jest zgodne z określonymi wcześniej wartościami referencyjnymi.

Tabl. 1. Rozkład liczby sygnałów autentycznych wykrywanych przed i po filtracji przestrzennej

Liczba sygnałów	Częstość przed filtracją przestrzenną	Częstość po filtracji przestrzennej
0	89,8%	0,0%
1	10,2%	2,0%
2	0,0%	14,6%
3	0,0%	47,6%
4	0,0%	25,4%
5	0,0%	10,0%
6	0,0%	0,4%

PODSUMOWANIE

Przedstawione wyniki badań pomiarowych potwierdzają, że zaproponowane rozwiązanie systemu antyspoofingowego może być z powodzeniem zastosowane do wykrywania i eliminacji spoofingu w systemie GPS, co ma szczególne znaczenie w przypadku zapewnienia bezpieczeństwa nawigacji morskiej.

Należy podkreślić, że, w przeciwieństwie do wielu konkurencyjnych rozwiązań, nie wymaga ono zewnętrznych źródeł informacji ani jakichkolwiek modyfikacji sygnałów nadawanych przez satelity nawigacyjne. Ponadto, przyjęta metoda detekcji spoofingu, oparta na porównywaniu opóźnień fazowych sygnałów, nie wymaga skomplikowanej kalibracji szyku antenowego.

Opracowany prototyp systemu może stanowić punkt wyjścia do realizacji wersji produkcyjnej. Wymagałoby to zastosowania innej platformy sprzętowej, bardziej odpowiedniej do realizacji złożonych obliczeniowo algorytmów cyfrowego przetwarzania sygnałów GPS. Taką platformą mogą być na przykład układy programowalne FPGA lub procesory kart graficznych.

Kwestią wymagającą przeprowadzenia bardziej szczegółowych badań jest działanie systemu w warunkach intensywnej propagacji wielodrogowej, gdzie odbite repliki sygnałów imitujących mogą docierać do odbiornika z różnych kierunków. W takim przypadku jest wskazana niezależna eliminacja poszczególnych składowych, co jednakże wymaga bardziej złożonego szyku antenowego.

LITERATURA

1. Divis D. A.: GPS Spoofing Experiment Knocks Ship off Course (http://www.insidegnss.com/node/3659), 2013.
2. Humphreys T.: Statement on the Vulnerability of Civil Unamnned Aerial Vehicles and Other Systems to Civil GPS Spoofing, 2012.
3. Jafarnia-Jahromi A., Broumandan A., Nielsen J., Lachapelle G.: GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. International Journal of Navigation and Observation, vol. 2012. doi:10.1155/2012/127072.
4. Kaplan E., Hegarty C.: Understanding GPS: Principles and Applications, Second Edition. Artech House mobile communications series. Artech House, 2005.
5. Magiera J., Katulski R.: Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. Journal of Applied Research and Technology, vol. 13 (nr 1), 2015, 45-57.
6. Mitch R. H.: Signal Characteristics of Civil GPS Jammers. ION GNSS, Portland, Oregon, 2011.
7. Sathyamoorthy D.: Global navigation satellite system (GNSS) spoofing: A review of growing risks and mitigation steps. Defence S&T Technical Bulletin, vol. 6 (nr 1), 2013, 42–61.
8. Shepard D. P., Bhatti J.A., Humphreys T.E.: 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), 2012. Nashville, USA, 3591-3605.
9. http://www.novatel.com/solutions/anti-jamming-technology/