Jarosław MAGIERA[1], Ryszard J. KATULSKI[1]

Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki, Katedra Systemów i Sieci Radiokomunikacyjnych (1)

doi:10.15199/48.2015.03.15

Analiza i badania systemu antyspoofingowego GPS

Streszczenie. *Artykuł dotyczy problemu spoofingu w systemie GPS, polegającego na niepowołanej transmisji sygnałów imitujących sygnały odbierane z satelitów GPS. Takie działanie prowadzi do wyznaczenia przez odbiornik nawigacyjny nieprawidłowego położenia, prędkości i czasu. Zostały opisane metody przeciwdziałania spoofingowi, w szczególności poprzez przestrzenne przetwarzanie sygnałów. Przedstawiono wyniki badań symulacyjnych efektywności tych metod. Opisano demonstrator sytemu antyspoofingowego i wybrane wyniki badań pomiarowych.*

Abstract*. The article concerns the problem of spoofing in GPS, which is the unauthorized transmission of signals imitating the ones received from GPS satellites. Such activity is aimed to force the estimation of incorrect position, velocity and time in a target GPS receiver. Authors review the anti-spoofing methods with the emphasis laid on spatial processing algorithms. Simulation research of the effectiveness of these methods is described. Proof-of-concept of the anti-spoofing system is shown along with the selected results of performed measurements. (**Analysis and research on anti-spoofing system for GPS**).*

Słowa kluczowe: GPS; Walka elektroniczna, Spoofing; Przestrzenne przetwarzanie sygnałów.
Keywords: GPS; Electronic warfare; Spoofing; Spatial signal processing.

Wstęp

Intencją powstania systemu nawigacji satelitarnej GPS było zastosowanie go w działaniach militarnych armii Stanów Zjednoczonych, m. in. do naprowadzania pocisków rakietowych. Ze względu na taki charakter zastosowań, podstawowe sygnały nawigacyjne P, odbierane przez urządzenia wojskowe, podlegają ochronie kryptograficznej. Oprócz sygnałów podstawowych satelity systemu nadają sygnały pomocnicze C/A, które skracają czas dostrojenia się odbiornika do sygnałów P. Wyznaczenie położenia odbiornika jest wprawdzie możliwe w oparciu o same sygnały C/A, jednakże możliwa do uzyskania dokładność położenia jest o rząd wielkości (do 2000 r. o dwa rzędy wielkości) mniejsza. Sygnały C/A są używane do wyznaczania położenia i czasu we wszystkich cywilnych odbiornikach GPS, wliczając w to odbiorniki pracujące w ramach infrastruktury krytycznej (m.in. w sieciach energetycznych i telekomunikacyjnych, transporcie itp.). W takich aplikacjach jest pożądane zapewnienie ciągłości i autentyczności odbieranych sygnałów nawigacyjnych. Tymczasem sygnały C/A nie są w żaden sposób zabezpieczone przed ich sfałszowaniem. Wszelkie parametry tych sygnałów, jak również struktura depeszy nawigacyjnej są opublikowane w powszechnie dostępnej specyfikacji interfejsu radiowego satelita-odbiornik [1]. Stwarza to możliwość przeprowadzenia ataku elektronicznego zwanego spoofingiem GPS.

Przez spoofing GPS rozumie się nieuprawnioną transmisję fałszywych sygnałów imitujących sygnały odbierane z satelitów systemu GPS. Urządzenie emitujące fałszywe sygnały jest nazywane spooferem. Celem takiego ataku jest doprowadzenie do sytuacji, w której odbiornik, zamiast prawdziwych informacji o położeniu, prędkości i czasie, będzie wskazywał wartości parametrów ustalone w spooferze. Takie działanie stanowi większe zagrożenie niż zwykłe zagłuszanie sygnału GPS, gdyż jest trudniejsze do wykrycia i powoduje wystąpienie informacji, która może być potencjalnie niebezpieczna dla użytkownika. W aplikacjach korzystających z sygnałów GPS C/A, wymagających zapewnienia wysokiego poziomu niezawodności i bezpieczeństwa, jest konieczne wdrożenie procedur skutecznej ochrony przed spoofingiem.

Badania zmierzające do wypracowania efektywnych metod przeciwdziałania spoofingowi w systemach GNSS (Global Navigation Satellite Systems), prowadzone w Katedrze Systemów i Sieci Radiokomunikacyjnych Politechniki Gdańskiej, mogą mieć znaczenie dla poprawy bezpieczeństwa w nawigacji, transporcie, telekomunikacji, energetyce i w wielu innych dziedzinach, w których znajduje zastosowanie system GPS.

Metody antyspoofingowe

Zabezpieczenie odbiornika GPS przed oddziaływaniem spoofingu wymaga implementacji sprzężonych algorytmów wykrywania spoofingu i jego eliminacji. Proponowane w literaturze metody wykrywania różnią się między sobą skutecznością, złożonością obliczeniową i stopniem ingerencji w budowę odbiornika [2]. Najprostsze, a zarazem najmniej efektywne metody detekcji bazują na analizie zależności czasowych oraz parametrów związanych z mocą odbieranych sygnałów. Przykładowo, obserwowane są zmiany mocy sygnału odbieranego podczas ruchu odbiornika lub jest mierzone względne opóźnienie pomiędzy sygnałami nadawanymi na różnych częstotliwościach. W innych metodach, monitorowany jest rozkład próbek maksimum funkcji korelacji w odbiorniku, jak również kształt tej funkcji. Nietypowe wskazania tych parametrów mogą świadczyć o obecności fałszywych sygnałów GPS. Bardziej skutecznym sposobem wykrywania spoofingu jest porównanie położenia wyznaczonego na podstawie sygnałów GPS z położeniem obliczonym przez odbiornik innego systemu nawigacyjnego. Należy się jednak liczyć z tym, że sygnały innego systemu radionawigacyjnego mogą być zakłócone, a, jeśli jest to system naziemny, to jego zasięg jest ograniczony terytorialnie. Innym skutecznym sposobem sprawdzenia, czy odbierane sygnały GPS są prawdziwe, mogłoby być wprowadzenie ich ochrony kryptograficznej z jednoczesnym zachowaniem wstecznej kompatybilności z dotychczas wyprodukowanymi odbiornikami. Proponowane rozwiązanie zakłada przesyłanie, w aktualnie nieużywanych polach depeszy, niemożliwego do sfałszowania podpisu cyfrowego. Zasadniczą wadą w tym przypadku jest konieczność wprowadzenia modyfikacji również po stronie nadawczej, co może być zrealizowane jedynie przez Departament Obrony Stanów Zjednoczonych. Skuteczną metodą detekcji spoofingu, wymagającą jedynie zmodyfikowania budowy odbiornika GPS, jest analiza przestrzenna odbieranych sygnałów. Sygnały nadawane przez satelity docierają do odbiornika z różnych kierunków. Z kolei spoofer nadaje wszystkie sygnały przez jedną antenę, co oznacza, że mają one taki sam kierunek nadejścia. Wykrycie co najmniej czterech sygnałów o zbliżonych do siebie kierunkach nadejścia może wskazywać na wystąpienie spoofingu.

Po wykryciu spoofingu należy zastosować procedurę ograniczenia lub całkowitego wyeliminowania jego wpływu na pracę odbiornika. Jeśli ciągła dostępność autentycznych sygnałów GPS nie jest krytyczna, wystarczy powiadomienie użytkownika o wystąpieniu spoofingu i zaprzestanie wyznaczania czasu i położenia. W przeciwnym wypadku należy podjąć próbę wyselekcjonowania sygnałów prawdziwych i odrzucenia fałszywych. Znanych jest stosunkowo niewiele metod realizacji tego zadania. Jedną z nich jest użycie algorytmu RAIM (ang. Receiver Autonomous Integrity Monitoring), który analizuje spójność odbieranych sygnałów pod kątem pseudoodległości i depesz nawigacyjnych, a następnie odrzuca sygnały niezgodne z większością pozostałych. Intencją zastosowania tego algorytmu było wykrywanie i odrzucanie sygnałów z nieprawidłowo działających satelitów GPS, jednakże można go też użyć, w ograniczonym zakresie, do przeciwdziałania spoofingowi. Inna metoda, o nazwie VSD (ang. Vestigial Signal Detection), czyli detekcja sygnału szczątkowego, zakłada, że odbierane sygnały spoofera mają tak dużą moc, że uniemożliwiają odbiór sygnałów prawdziwych. Metoda ta ma dwa etapy. W pierwszym odbierane są silne, uznawane za fałszywe, sygnały GPS i tworzone są ich repliki. W drugim etapie te repliki są odejmowane od opóźnionej wersji całkowitego sygnału odbieranego. W uzyskanym sygnale szczątkowym są poszukiwane słabsze sygnały GPS, pochodzące z satelitów. Inne podejście do kwestii eliminacji spoofingu zakłada zastosowanie filtracji przestrzennej sygnałów, tzw. kształtowania zer (ang. null steering). Stosowany jest w tym przypadku odbiór wieloantenowy, a charakterystykę odbiorczą kształtuje się tak, aby uzyskać silne tłumienie sygnału z określonego kierunku. Znając kierunek nadejścia sygnałów spoofera, można wysterować szyk antenowy tak, aby tłumić te sygnały, a jednocześnie umożliwić odbiór sygnałów z satelitów.

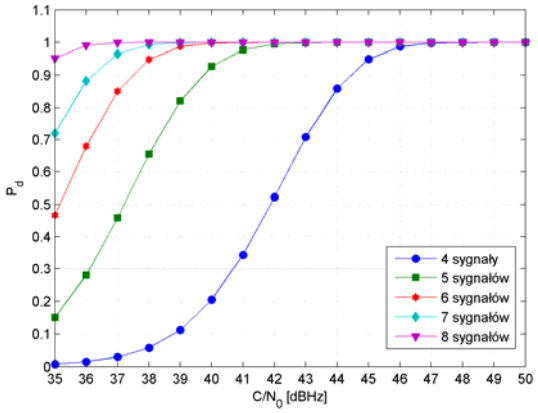
Efektywność przetwarzania przestrzennego

Aktualnie najbardziej niezawodnymi metodami wykrywania i eliminacji spoofingu są te, które bazują na przestrzennym przetwarzaniu sygnałów. Jest to spowodowane tym, że nie jest możliwe zdefiniowanie przez spoofer różnych kierunków nadejścia dla poszczególnych sygnałów fałszywych.

W ramach prac prowadzonych w Katedrze Systemów i Sieci Radiokomunikacyjnych Politechniki Gdańskiej (KSiSR PG) zbadano efektywność tych metod na drodze symulacji komputerowych. Przyjęto tu model układu antenowego złożonego z czterech elementów rozmieszczonych w wierzchołkach kwadratu o długości boku równej 0,45 długości fali o częstotliwości 1575,42 MHz.

Badana metoda detekcji spoofingu różni się od opisywanej w poprzednim rozdziale. Nie są tu porównywane kierunki nadejścia poszczególnych sygnałów GPS, lecz ich opóźnienia fazowe mierzone pomiędzy wybranymi elementami układu antenowego. Takie rozwiązanie ma dwie zalety. Po pierwsze, nie jest wymagana kalibracja fazowa układu antenowego i torów sygnałowych w.cz. Po drugie, błąd estymacji kierunku nadejścia sygnału zależy od tego kierunku i konfiguracji geometrycznej elementów antenowych. W przypadku błędu opóźnień fazowych taka zależność nie występuje. Stwierdzono, że błąd estymacji opóźnień fazowych można opisać rozkładem normalnym o zerowej wartości średniej i wariancji uzależnionej od stosunku mocy sygnału do mocy szumu.

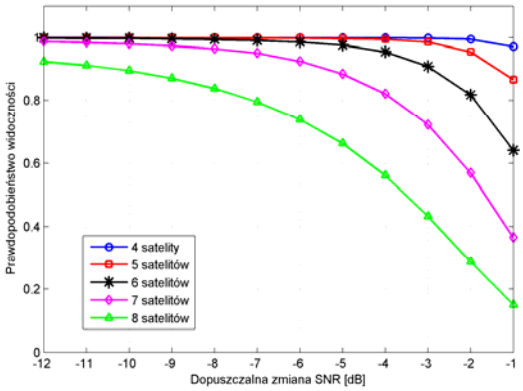
Efektywność metod detekcji spoofingu można opisać prawdopodobieństwami: detekcji i fałszywego alarmu. Pierwsze mówi o tym, jak często zostanie wykryty spoofing faktycznie występujący. Z kolei drugie daje informację jak często zostanie podjęta pozytywna decyzja o detekcji w przypadku braku spoofingu. Oba są uzależnione od progu detekcji, który powinien zostać dobrany w taki sposób, aby uzyskać akceptowalnie małe prawdopodobieństwo fałszywego alarmu P_{FA} i jak największe prawdopodobieństwo detekcji P_D. Próg detekcji oznacza w tym przypadku taką wartość różnic opóźnień fazowych pomiędzy co najmniej czterema sygnałami GPS, poniżej której uznaje się, że sygnały te docierają z tego samego kierunku, a więc spoofing jest obecny. Oprócz progu detekcji, czynnikami wpływającymi na wartości prawdopodobieństw są: liczba odbieranych sygnałów oraz ich jakość. Jakość każdego sygnału jest określona stosunkiem C/N_0, czyli mocy fali nośnej sygnału odniesionej do widmowej gęstości mocy szumu i interferencji. W prowadzonych badaniach symulacyjnych przyjęto, że P_{FA} nie może przekraczać wartości 10^{-4}. Dla takiego założenia wyznaczono wartości progów detekcji dla przypadków odbioru od czterech do ośmiu sygnałów i dla zakresu C/N_0 od 35 dBHz do 60 dBHz, który odpowiada wartościom obserwowanym w warunkach rzeczywistych. Dla wyznaczonych progów detekcji oszacowano prawdopodobieństwo poprawnej detekcji spoofingu. Wyniki zostały zaprezentowane na rysunku 1. Dla wartości C/N_0 nie mniejszych niż 40 dBHz, przy odbiorze co najmniej pięciu fałszywych sygnałów, prawdopodobieństwo detekcji jest większe od 0,9. W przypadku odbioru tylko czterech sygnałów takie prawdopodobieństwo uzyskuje się przy C/N_0 co najmniej równym 45 dBHz. Bardziej szczegółowy opis badań detekcji spoofingu można znaleźć w [3].



Rys.1. Prawdopodobieństwo wykrycia spoofingu

Efektywność metod eliminacji spoofingu można wyrazić prawdopodobieństwem możliwości odbioru określonej liczby prawdziwych sygnałów GPS w obecności spoofingu. Przyjęta metoda filtracji przestrzennej poprzez kształtowanie zer charakterystyki umożliwia silne wytłumienie wszystkich fałszywych sygnałów docierających z danego kierunku, jednakże wpływa także na jakość docierających z satelitów sygnałów prawdziwych. Proces filtracji może spowodować spadek stosunku sygnał-szum, co z kolei może uniemożliwić odbiór tego sygnału. Przyjmując pewną dopuszczalną wartość tego spadku i znając położenie satelitów widocznych w danej chwili i miejscu na Ziemi a także kierunek nadejścia sygnałów fałszywych, można dokonać oszacowania prawdopodobieństwa możliwości odbioru określonej liczby sygnałów prawdziwych. Taka analiza została przeprowadzona, a jej wyniki przedstawiono na rysunku 2. Przykładowo, jeśli dopuszcza się na wyjściu filtru przestrzennego spadek stosunku sygnał-szum o nie więcej

niż 3 dB, to prawdopodobieństwa możliwości odbioru od 4 do 8 sygnałów z satelitów wynoszą odpowiednio: 99,9%, 98,6%, 90,9%, 72,3% i 43,3%. Dokładniejszy opis badań eliminacji spoofingu poprzez filtrację przestrzenną można znaleźć w [4].



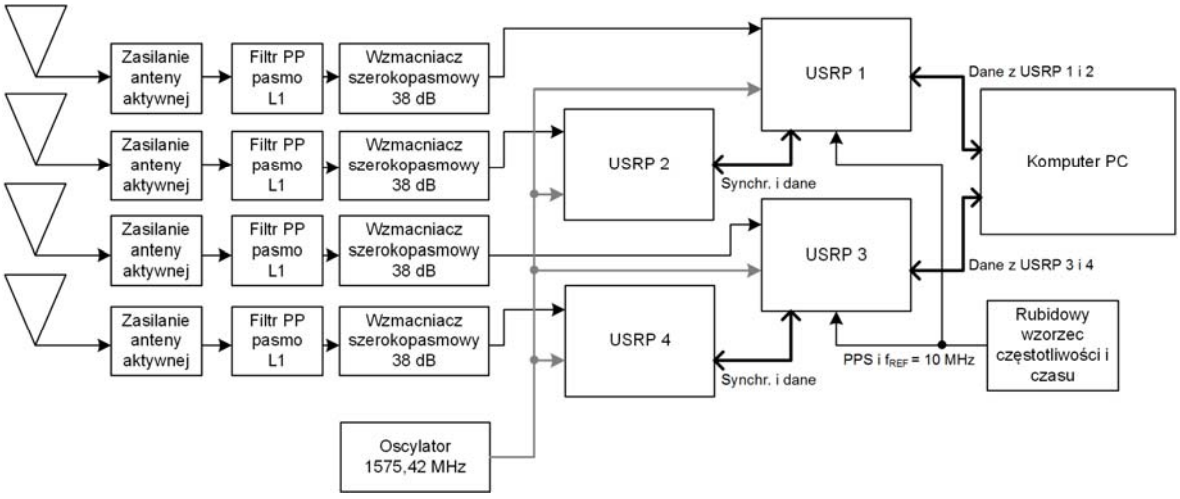
Rys.2. Prawdop. możliwości odbioru danej liczby sygnałów

Demonstrator systemu antyspoofingowego

Na podstawie wyników badań symulacyjnych można określić efektywność proponowanych rozwiązań w warunkach modelowych. Właściwa ocena efektywności wymaga przeprowadzenia testów systemu w warunkach rzeczywistych. Dlatego też, w KSiSR PG został opracowany demonstrator systemu.

Przy realizacji demonstratora zdecydowano się zastosować technikę radia programowalnego SDR (ang. software defined radio), co oznacza, że liczba analogowych bloków odbiornika jest ograniczona do minimum, a zasadnicze przetwarzanie sygnałów jest realizowane po stronie oprogramowania. W części analogowej zastosowano czteroelementowy szyk antenowy, tak jak zdefiniowano go w modelu symulacyjnym. Sygnały z wyjść anten podlegają filtracji pasmowo-przepustowej oraz wzmocnieniu o 38 dB. Następnie te sygnały są podane na wejścia urządzeń USRP (ang. Universal Software Radio Peripheral) model NI USRP-2920 [5], które realizują przeniesienie sygnałów z pasma w.cz. do pasma podstawowego oraz przetwarzają je z postaci analogowej na cyfrową. Urządzenia USRP są synchronizowane przy użyciu rubidowego wzorca częstotliwości, a przesunięcia fazowe ich oscylatorów lokalnych są mierzone w oparciu o sygnał z oscylatora referencyjnego, a następnie kompensowane. Próbki sygnałów są przesyłane z USRP do komputera PC, który realizuje algorytmy antyspoofingowe. Użyta platforma sprzętowa została przedstawiona na rysunku 3., a schemat blokowy demonstratora systemu na rysunku 4. Aktualnie demonstrator jest używany do celów badawczych – do pomiaru: charakterystyk błędu estymacji opóźnień fazowych, prawdopodobieństwa detekcji spoofingu i efektywności filtracji przestrzennej sygnałów niepożądanych.

Rys.3. Platforma sprzętowa demonstratora systemu antyspoofingowego (szyk antenowy, tory w.cz, urządzenia USRP i wzorzec rubidowy)

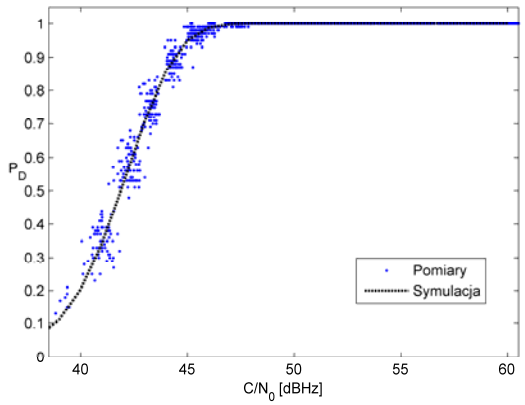


Rys.4. Schemat blokowy demonstratora systemu antyspoofingowego

Wyniki badań pomiarowych

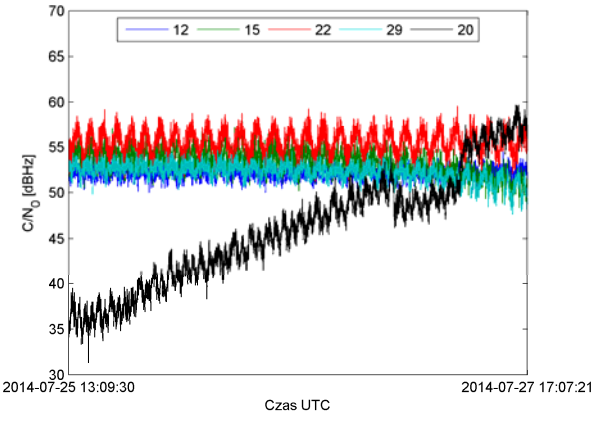
Poniżej zaprezentowano wybrane wyniki badań pomiarowych, przeprowadzonych z użyciem opracowanego demonstratora.

Na rysunku 5. przedstawiono uzyskane wyniki pomiaru prawdopodobieństwa detekcji (niebieskie punkty) dla przypadku odbioru czterech fałszywych sygnałów. Linią przerywaną oznaczono rezultat badań symulacyjnych. Jak można zauważyć wyniki pomiarów są zbieżne z symulacją.

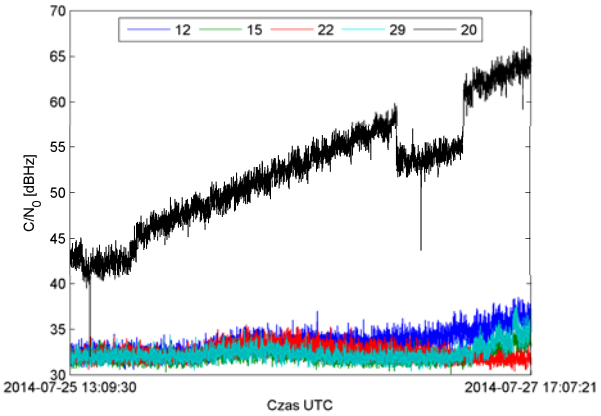


Rys.5. Wyniki pomiarów prawdopodobieństwa detekcji

Wyniki pomiarów efektywności filtracji przestrzennej są przedstawione na rysunkach 6. i 7. W konfiguracji pomiarowej cztery sygnały fałszywe, o numerach 12, 15, 22 i 29 były wytwarzane w generatorze i transmitowane przewodowo, poprzez dzielnik mocy, na wejścia w.cz. systemu antyspoofingowego. Z kolei sygnał o numerze 20, imitujący sygnał prawdziwy, był także wytwarzany w generatorze, lecz transmitowany bezprzewodowo i odbierany przez szyk antenowy. Na rysunkach zamieszczono wykresy przebiegów czasowych C/N_0 odbieranych sygnałów odpowiednio przed i po filtracji przestrzennej. Przed filtracją, C/N_0 czterech sygnałów fałszywych było na stałym poziomie, większym od 50 dBHz. Z kolei moc sygnału prawdziwego była stopniowo zwiększana w trakcie badania tak, aby uzyskać różne wartości C/N_0 sygnału prawdziwego od ok. 35 dBHz do ok. 57 dBHz. Po filtracji przestrzennej stosunki C/N_0 sygnałów fałszywych zmniejszyły się do wartości nieznacznie przekraczających 30 dBHz, co odpowiada praktycznie całkowitemu wytłumieniu tych sygnałów. Natomiast odnotowano wzrost C/N_0 sygnału prawdziwego o ok. 7 dB do 10 dB, w stosunku do wartości przed filtracją.



Rys.6. C/N_0 odbieranych sygnałów GPS przed filtr. przestrzenną



Rys.7. C/N_0 odbieranych sygnałów GPS po filtr. przestrzennej

Podsumowanie

W artykule opisano spoofing, jako możliwe zagrożenie bezpieczeństwa korzystania z odbiorników systemu nawigacji satelitarnej GPS. Celowe wprowadzanie błędnych informacji o położeniu i czasie jest szczególnie niebezpieczne dla funkcjonowania elementów infrastruktury krytycznej. W obliczu takiego zagrożenia uzasadnioną jest implementacja dodatkowych mechanizmów ochronnych w odbiornikach GPS. Spośród wymienionych metod wykrywania i eliminacji spoofingu, metody oparte na przestrzennym przetwarzaniu sygnałów jawią się jako najbardziej skuteczne. Zarówno badania symulacyjne, jak i pomiary wskazują, że metody te mogą z powodzeniem znaleźć zastosowanie w systemie antyspoofingowym. Aktualnie w dalszym ciągu prowadzone są badania pomiarowe, mające na celu ocenę efektywności przyjętych rozwiązań w różnych warunkach propagacji sygnałów.

Opisane zagadnienie ma znaczenie praktyczne w obszarze bezpieczeństwa, m.in. w nawigacji, transporcie, telekomunikacji i energetyce.

LITERATURA

[1] GPS Directorate Systems Engineering & Integration. Interface Specification IS-GPS-200H: Navstar GPS Space Segment/Navigation User Interfaces. 2014.

[2] 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.

[3] Magiera J., Katulski R., *Accuracy of Differential Phase Delay Estimation for GPS Spoofing Detection*. Materiały konf. 36th International Conference on Telecommunications and Signal Processing, Rzym, 07/2013, s. 695-699.

[4] Magiera J., Katulski R., *Applicability of null-steering for spoofing mitigation in civilian GPS*. Materiały konf. IEEE 79th Vehicular Technology Conference VTC 2014 Spring, Seul, 05/2014.

[5] National Instruments, NI USRP-292x/293x *Datasheet – Universal Software Radio Peripherals*, http://sine.ni.com/ds/app/doc/p/id/ds-355/lang/pl

***Autorzy**: mgr inż. Jarosław Magiera, Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki, ul. Narutowicza 11/12, 80-233 Gdańsk, E-mail: jaroslaw.magiera@eti.pg.gda.pl; prof. dr hab. inż. Ryszard J. Katulski, Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki, ul. Narutowicza 11/12, 80-233 Gdańsk, E-mail: rjkat@eti.pg.gda.pl.*