Technika ochrony odbiorników GPS
przed atakami typu spoofing

Jarosław Magiera, Ryszard Katulski

Artykuł został poświęcony problemowi tzw. spoofingu w systemach nawigacji satelitarnej GNSS. Mianem spoofingu GNSS określa się niepowołaną transmisję sygnałów GNSS, imitujących sygnały nadawane z satelitów nawigacyjnych. Celem takiego działania jest doprowadzenie do wskazania przez odbiornik GNSS nieprawidłowych informacji o położeniu, prędkości i czasie. Przeprowadzenie takiego ataku jest możliwe wskutek braku odpowiedniej ochrony integralności cywilnych sygnałów GNSS. Spoofing stanowi duże zagrożenie dla infrastruktury krytycznej, korzystającej z nawigacji satelitarnej, w tym portów lotniczych. Ochrona odbiorników GNSS przed spoofingiem ma szczególne znaczenie w związku z wprowadzeniem, w kwietniu 2013r., na 10 największych polskich lotniskach, procedur podejścia do lądowania w oparciu o nawigację satelitarną. W artykule przedstawiono metody wykrywania i przeciwdziałania spoofingowi w systemie GPS oparte na przestrzennym przetwarzaniu sygnałów. Analiza efektywności tych metod stanowi aktualny temat badań prowadzonych przez autorów.

mgr inż.
Jarosław Magiera
Politechnika Gdańska,
Wydział Elektroniki, Telekomunikacji i Informatyki,
Katedra Systemów i Sieci Radiokomunikacyjnych
jaroslaw.magiera@eti.pg.gda.pl

prof. dr hab. inż. , prof. nadzw. PG
Ryszard Katulski
Politechnika Gdańska,
Wydział Elektroniki, Telekomunikacji i Informatyki,
Katedra Systemów i Sieci Radiokomunikacyjnych
rjkat@eti.pg.gda.pl

Systemy GNSS i ich bezpieczeństwo

Globalne systemy nawigacji satelitarnej (ang. GNSS – Global Navigation Satellite Systems) są powszechnie stosowane w transporcie lądowym, morskim i lotniczym, ale również w innych dziedzinach, takich jak m.in.: geodezja, telekomunikacja, energetyka, rolnictwo i przemysł. Do grupy systemów GNSS należą: amerykański GPS, rosyjski GLONASS, chiński Beidou oraz satelitarne i naziemne systemy wspomagające, takie jak WAAS czy EGNOS. Od wielu lat trwają również prace nad wdrożeniem systemu Galileo, kontrolowanego przez Unię Europejską. Pomimo pełnej zdolności operacyjnej konstelacji systemu GLONASS, znacząca większość cywilnych odbiorników nawigacji satelitarnej korzysta z sygnałów nadawanych przez satelity GPS. Dlatego też, w niniejszym artykule skupiono się właśnie na tym systemie, jakkolwiek poruszane tutaj kwestie odnoszą się również do pozostałych przedstawicieli grupy GNSS.

Geneza systemu GPS była rezultatem potrzeby opracowania dokładnego systemu nawigacji satelitarnej dla armii Stanów Zjednoczonych. Z uwagi na to, że miał być to system do zastosowań militarnych, sygnały używane do określania położenia są zabezpieczone przed niepowołanym dostępem. Zabezpieczenie to polega na mnożeniu sygnałów przez pseudolosową sekwencję impulsów bipolarnych (tzw. ciąg P(Y)), która to sekwencja jest znana jedynie użytkownikom autoryzowanym. Demodulacja sygnału przez odbiornik GPS jest możliwa dopiero po uzyskaniu synchronizacji z odbieranym ciągiem P(Y). Czas nadawania jednego przebiegu sekwencji wynosi aż 7 dni, co w praktyce uniemożliwia dostrojenie się odbiornika. Dlatego też, oprócz sygnałów z ciągiem P(Y), satelity nadają drugi rodzaj sygnałów z tzw. ciągiem C/A (ang. Coarse Acquisition – zgrubna akwizycja). Ciąg C/A jest powtarzany co 1 milisekundę, co umożliwia łatwe dostrojenie odbiornika i uzyskanie informacji o aktualnym czasie systemowym. To, z kolei, ułatwia ustalenie aktualnej fazy ciągu P(Y). Obecność sygnałów z ciągami C/A ma kluczowe znaczenie dla użycia systemu GPS w zastosowaniach cywilnych. To właśnie na podstawie tych sygnałów ustalane jest położenie i czas we wszystkich ogólnodostępnych odbiornikach GPS na świecie.

Korzystając z nawigacji satelitarnej, użytkownicy zwykle nie przywiązują dużej wagi do bezpieczeństwa usługi oferowanej przez system. Gdy jest mowa o ryzyku związanym z używaniem systemu GPS, zazwyczaj rozumie się przez to wyznaczenie nieprawidłowej trasy przez oprogramowanie mapowe zainstalowane w odbiorniku. Jednakże bardziej istotną kwestią bezpieczeństwa wydaje się być wiarygodność i integralność odbieranych sygnałów nawigacyjnych. W przeciwieństwie do militarnych sygnałów P(Y), sygnały z ciągami C/A nie są w żaden sposób zabezpieczone kryptograficznie. Ponadto, postaci wszystkich ciągów C/A, jak również parametry czasowo-częstotliwościowe sygnałów oraz zawartość wiadomości nawigacyjnych, są podane do ogólnej wiadomości w specyfikacji interfejsu radiowego satelita-odbiornik [X]. Stwarza to możliwość wytworzenia własnych sygnałów GPS o zadanych parametrach. Jest to korzystne z punktu widzenia możliwości testowania odbiorników w ściśle zdefiniowanych i powtarzalnych warunkach, jednakże wprowadza także niebezpieczeństwo wystąpienia ataku zwanego spoofingiem GPS.

Spoofing w systemie GNSS można zdefiniować jako rodzaj ataku elektronicznego, w którym do odbiornika docierają sfałszowane sygnały, imitujące sygnały odbierane z satelitów GPS. Nadajnik emitujący tego typu sygnały jest nazywany spooferem. Celem spoofingu jest doprowadzenie do sytuacji, w której odbiornik, zamiast prawdziwych informacji o pozycji, prędkości i czasie, będzie wskazywał wartości parametrów ustalone w spooferze. Spoofing można uznać za bardziej wyrafinowaną formę zagłuszania sygnału. Sygnał spoofera nie tylko uniemożliwia odbiór sygnałów z satelitów GPS, ale także dostarcza nieprawidłowych wskazań, co jest potencjalnie niebezpieczne.

Niepowołana transmisja jakichkolwiek sygnałów w pasmie zarezerwowanym dla systemów radionawigacyjnych jest niezgodna z prawem. Obecność takiej transmisji stwarza szczególne zagrożenie dla bezpieczeństwa nawigacji i funkcjonowania infrastruktury krytycznej. Należy pamiętać, że systemy GNSS nie są używane wyłącznie do ustalania położenia, ale także do synchronizacji sieci rozproszonych urządzeń, jakimi są np. telekomunikacyjne sieci komórkowe lub sieci elektroenergetyczne. Zaburzenia pracy takich sieci mogą powodować duże straty materialne.

W ostatnim czasie, zapewnienie ciągłości i poprawności sygnałów nawigacji satelitarnej nabrało szczególnego znaczenia dla transportu lotniczego. Ma to związek z wprowadzaniem na lotniskach europejskich procedur podejścia do lądowania w oparciu o wskazania instrumentów GNSS. Chodzi tu przede wszystkim o system GPS i wspomagający go satelitarny geostacjonarny system EGNOS. Procedury takie wprowadziły m.in. Niemcy i Francja. W Polsce wdrożenie procedur na 10 największych lotniskach przeprowadzono w kwietniu 2013 roku.

Wykrywanie obecności spoofingu

W przeciwieństwie do wykrycia zagłuszania (ang. jamming), detekcja wystąpienia spoofingu nie jest zadaniem trywialnym. W przypadku zagłuszania odbiornik nie jest w stanie zdemodulować żadnych sygnałów GPS, co skutkuje zaprzestaniem wyznaczania czasu systemowego i położenia. Z kolei odbiornik poddany działaniu spoofingu , nie wyposażony w dodatkowe mechanizmy ochronne, będzie pracował normalnie – wskazując nieprawidłowe wartości parametrów lokalizacyjnych.

Spoofing może zostać przeprowadzony w taki sposób, że przestrojenie się odbiornika z odbioru sygnałów prawdziwych na fałszywe będzie niezauważalne. W takim scenariuszu, początkowe położenie, obliczone na bazie sygnałów fałszywych jest takie samo jak rzeczywiste położenie odbiornika. Moc sygnałów fałszywych jest stopniowo zwiększana, aby wymusić dostrojenie się do nich odbiornika, stanowiącego cel ataku. Następnie, poprzez sterowanie zależnościami czasowymi sygnałów, fałszywa pozycja jest oddalana od prawdziwej, aby ostatecznie wskazać współrzędne zadane przez operatora spoofera.

W literaturze są proponowane różne podejścia do rozwiązania problemu wykrycia spoofingu GPS. Dobór odpowiedniej metody jest podyktowany możliwościami obliczeniowymi odbiornika. Najmniej złożone obliczeniowo są metody bazujące na analizie parametrów związanych z mocą lub zależnościami czasowymi odbieranych sygnałów. Jednakże efektywność takich rozwiązań jest stosunkowo niewielka, gdyż tego rodzaju parametry mogą być najczęściej zdefiniowane tak, aby ich wartości nie odbiegały od wartości obserwowanych w przypadku odbioru sygnałów z satelitów.

Inną propozycją jest porównywanie wskazań wyznaczonej pozycji z położeniem wyznaczonym przy użyciu innego systemu nawigacyjnego, jednakże należy w tym przypadku wziąć pod uwagę ograniczenia terytorialne (naziemne systemy radionawigacyjne) lub problematyczną kalibrację (systemy inercyjne).

Ponadto, postulowano wprowadzenie zabezpieczeń kryptograficznych do wiadomości nawigacyjnych zawartych w cywilnych sygnałach GPS. Polegałoby to na wyznaczeniu podpisanego cyfrowo skrótu przesyłanej depeszy nawigacyjnej, który pozwoliłby zweryfikować, czy jest ona oryginalna. Skrót byłby przesyłany w polach wiadomości, które nie są aktualnie używane, co pozwoliłoby zachować kompatybilność wsteczną ze wszystkimi wyprodukowanymi dotychczas odbiornikami. Niedogodnością tego rozwiązania jest konieczność wprowadzania zmian po stronie nadawczej, co wymaga działań ze strony organów nadzorujących działanie systemu satelitarnego.

Jedną z najskuteczniejszych metod detekcji spoofingu jest analiza kierunku nadejścia sygnałów. W sytuacji gdy sygnały odbierane są z satelitów GPS w warunkach bezpośredniej widoczności, ich kierunki nadejścia do anteny odbiorczej są różne. Inaczej jest w przypadku spoofingu, gdzie wszystkie wytwarzane sygnały są transmitowane z użyciem tej samej anteny nadawczej. Co za tym idzie, ich kierunki nadejścia są takie same. Aby określić kierunek nadejścia sygnału należy użyć układu kilku anten (szyku antenowego) i zmierzyć względne opóźnienia fazowe sygnałów docierających do poszczególnych anten. Do wyznaczenia położenia przez odbiornik jest wymagany odbiór co najmniej czterech sygnałów GPS. Zatem można wnioskować, że spoofing jest obecny, gdy wartości opóźnień fazowych, związane z co najmniej czterema sygnałami GPS, są do siebie zbliżone. Próg detekcji, czyli wartość różnicy opóźnień fazowych sygnału, poniżej której podejmuje się pozytywną decyzje o wykryciu spoofingu, jest uzależniony od liczby odbieranych fałszywych sygnałów oraz od ich jakości, wyrażanej parametrem C/N0. Mierzone w warunkach rzeczywistych wartości tego parametru zawierają się w granicach od 35 dBHz do 60 dBHz. Najbardziej czułe odbiorniki mogą wykrywać sygnały o C/N0 już od 30 dBHz, jednak po demodulacji ich przebieg jest zbliżony do szumu. Możliwe do uzyskania prawdopodobieństwo detekcji spoofingu jest tym większe im więcej fałszywych sygnałów jest odbieranych i im większa jest wartość ich C/N0. Na rys. X przedstawiono uzyskane symulacyjnie wartości prawdopodobieństwa detekcji spoofingu w funkcji C/N0 dla przypadków odbioru od czterech do ośmiu fałszywych sygnałów.

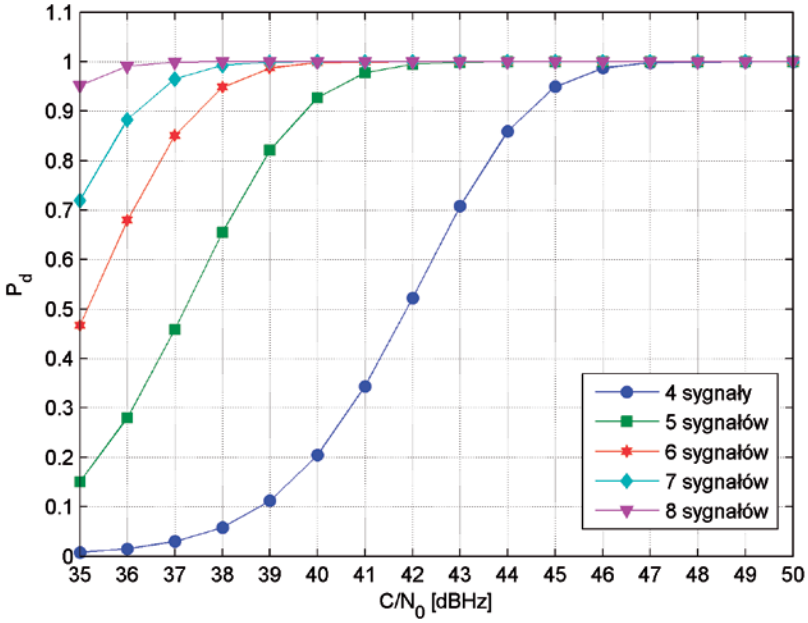
Przeciwdziałanie spoofingowi

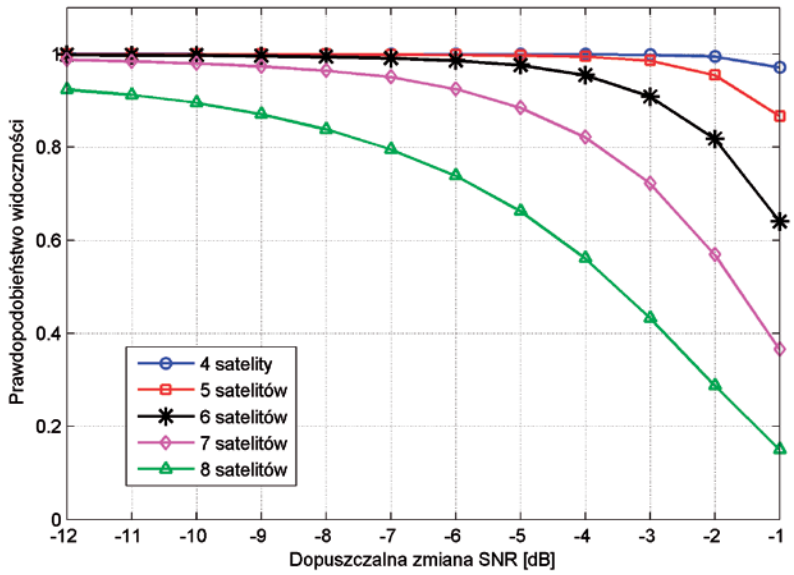
Wykrycie spoofingu jest pierwszym etapem procedury antyspoofingowej. Kolejnym krokiem jest ograniczenie wpływu działania spoofingu na pracę odbiornika GPS. Najprostszym rozwiązaniem jest powiadomienie użytkownika o wystąpieniu ataku i przerwanie wyznaczania parametrów lokalizacyjnych do chwili aż odbiornik znajdzie się poza zasięgiem oddziaływania spoofera. Oczywiście takie rozwiązanie jest możliwe jedynie w przypadkach gdzie ciągła dostępność sygnałów nawigacyjnych nie jest wymagana. W pozostałych przypadkach należy dokonać próby eliminacji fałszywych sygnałów.

W przeciwieństwie do metod wykrywania spoofingu, liczba znanych metod eliminacji fałszywych sygnałów jest stosunkowo niewielka. Podstawowym problemem przy takim działaniu jest sposób odseparowania sygnałów fałszywych od prawdziwych. Nie jest to możliwe do uzyskania poprzez filtrację częstotliwościową , gdyż oba rodzaje sygnałów są przesyłane dokładnie w tym samym pasmie.

Jedna z metod eliminacji spoofingu zakłada użycie algorytmu monitorowania przez odbiornik integralności sygnałów GPS. Ten algorytm o nazwie RAIM (ang. Receiver Autonomous Integrity Monitoring), analizuje depesze nawigacyjne i czasy propagacji sygnałów od poszczególnych satelitów. W przypadku stwierdzenia wzajemnej niezgodności sygnałów, te z nich, które nie są zgodne z większością, nie są uwzględniane przy wyznaczaniu położenia odbiornika. Pierwotnym zastosowaniem tego algorytmu jest wykluczenie sygnałów satelitów, które nie funkcjonują prawidłowo. Jednakże, w pewnych warunkach, może być on użyty do przeciwdziałania spoofingowi GPS.

Inną metodą jest detekcja sygnału szczątkowego VSD (ang. Vestigial Signal Detection). Odbiór sygnałów GPS jest w tym przypadku realizowany dwuetapowo. W pierwszej fazie są tworzone repliki wszystkich sygnałów GPS, które zostały wykryte. Zakłada się, że są to sygnały fałszywe, których moc jest na tyle duża, że uniemożliwia odbiór sygnałów prawdziwych. Następnie repliki są odejmowane od odpowiednio opóźnionego całkowitego sygnału docierającego do wejścia odbiornika. W wyniku tego odejmowania uzyskiwany jest sygnał szczątkowy. W wypadku braku spoofingu, sygnał szczątkowy składa się jedynie z szumów i ewentualnych interferencji. Z kolei w warunkach oddziaływania spoofingu sygnał szczątkowy może zawierać prawdziwe sygnały z satelitów GPS. Metoda VSD przypomina metodę redukcji





interferencji wynikających z wielodostępu w systemach komórkowych trzeciej generacji (UMTS). Można określić mianem eliminacji spoofingu w dziedzinie czasu. Zasadniczą wadą takiego rozwiązania jest wymóg, aby sygnały spoofera były znacznie silniejsze od sygnałów prawdziwych.

Takie ograniczenia nie występują w przypadku metody realizującej eliminację sygnałów na podstawie kierunku ich nadejścia. Przy użyciu odbioru wieloantenowego jest możliwe takie ukształtowanie charakterystyki odbiorczej, aby wszystkie sygnały docierające z określonego kierunku były silnie stłumione. Takie podejście jest nazywane kształtowaniem zer charakterystyki układu antenowego. W przypadku układu składającego się z M anten jest możliwe zdefiniowanie maksymalnie M-1 zer, czyli kierunków na których sygnały mają być tłumione. Jednakże w takim przypadku występuje także niepożądane tłumienie na innych kierunkach (rys. X). Można jednak również dobrać współczynniki w taki sposób, aby ustalić jedno zero na wybranym kierunku (rys. X). Ustalenie kilku zer charakterystyki jest zasadne jedynie w przypadku propagacji wielodrogowej, gdy do odbiornika dociera kilka kopii sygnału spoofera, powstałych w wyniku odbić od przeszkód na trasie transmisji.

Efektywność metod antyspoofingowych stosujących odbiór wieloantenowy

Aby dokonać oceny efektywności metody antyspoofingowej należy zdefiniować zestaw uniwersalnych parametrów jakościowych, których wartości mogą być wyznaczone dla dowolnej metody i, na podstawie których metody mogą być porównane. ◀