TECHNIKA TRANSPORTU SZYNOWEGO

Piotr KOWALECZKO, Jarosław SULKOWSKI

ANALIZA MOŻLIWOŚCI REALIZACJI ATAKU SPOOFINGU, CZYLI ŚWIADOMEGO ODDZIAŁYWANIA NA PRACĘ ODBIORNIKA SYSTEMU NAWIGACJI SATELITARNEJ GPS

Streszczenie

W pracy przedstawiono wyniki prowadzonych w ITWL badań nad możliwością generowania sygnałów emitowanych przez satelity systemu nawigacji satelitarnej GPS. Odebranie przez odbiornik co najmniej 4 odpowiednio spreparowanych sygnałów tego typu daje możliwość wyprowadzenia go z poprawnej pracy – dokonania ataku spoofing'owego. Omówiono metody generowania pojedynczego sygnału z wykorzystaniem jednego generatora częstotliwości nośnej (jeden kanał), dwóch sygnałów z wykorzystaniem dwóch generatorów (dwa kanały), oraz metody generowania wielu sygnałów przy wykorzystaniu pojedynczego generatora (kanał współdzielony).

WSTĘP

Globalne systemy nawigacji satelitarnej (GNSS) odgrywają obecnie niezwykle ważną rolę w wielu dziedzinach działalności człowieka. Są wykorzystywane zarówno w obronności czy ratownictwie, jak i w geodezji, logistyce czy transporcie. Nie są one jednak systemami wolnymi od wad. Stosunkowo łatwo jest je bowiem wyprowadzić z poprawnej pracy.

Zakłócanie systemu GPS polega na uniemożliwieniu odbiornikowi prawidłowego określenia parametrów pozycji, czasu i nawigacyjnych (PNT – position, navigation, time). Jest to możliwe poprzez ingerencję w docierające do odbiornika sygnały. Najpowszechniej stosowanymi metodami zakłócania odbiorników GPS są zagłuszanie i fałszowanie sygnału. Celem tego typu działań może być, bądź to uniemożliwienie jakiegokolwiek wyznaczenia parametrów PNT (zagłuszanie, jamming), bądź też fałszowanie informacji tak, aby parametry PNT wyznaczono błędnie (spoofing). W dalszej części przedstawiona zostanie metoda generacji kodów identyfikacyjnych satelitów systemu GPS, będąca podstawą do przeprowadzenia spoofing'u.

1. SPOOFING

O ile w przypadku blokowania i zagłuszania odbiorników systemu GPS (jamming) użytkownik jest świadomy nieprawidłowej pracy systemu ze względu na utratę sygnału, to w przypadku spoofing'u możemy mówić o ataku „ukrytym", na który odbiorniki mogą być nieodporne [1]. Co więcej, użytkownik nie ma świadomości że dane urządzenie wyznacza nieprawidłowe parametry PNT.

Czym zatem jest spoofing? Ogólna definicja tego zjawiska obejmuje szeroki zakres ataków sieci komputerowej w której atakujący próbuje fałszować dane lub ingerować w strumień danych [2]. Fałszowanie danych może odnosić się na przykład do wprowadzania przekłamań źródłowego adresu IP (IP spoofing) w wysyłanym przez komputer pakiecie sieciowym, co może posłużyć na przykład do podszycia się pod innego użytkownika sieci i korzystania z jego uprawnień [3]. Spoofing'iem można także nazwać ataki polegające na wprowadzaniu przekłamań w danych identyfikacyjnych uczestników rozmów telefonicznych (zarówno GSM jak i VoIP), zmianie adresu nadawcy wiadomości e-mail (wykorzystywaną często przez spamm'erów), czy też ataki wykorzystujące przechwytywanie danych przeznaczonych dla innego użytkownika sieci (ARP spoofing) [4]. Definicja odnosząca się bezpośrednio do systemu GPS mówi o fałszowaniu danych, które są porównywane w procesie replikacji kodu GPS, a w konsekwencji błędnym wyznaczaniu na ich podstawie parametrów PNT, błędnym rozwiązaniu. Mówiąc o spoofingu możemy wyróżnić trzy rodzaje oddziaływania w celu obniżenia dokładności i jakości otrzymanych wartości parametrów PNT:

- Programowe fałszowanie kodu – najbardziej inwazyjne, gdzie do odbiornika wprowadzany jest program typu malware (z ang. *malicious software*), czyli wszelkie aplikacje, skrypty, itp. mające szkodliwe, przestępcze lub złośliwe działanie w stosunku do użytkownika komputera. Odbiornik wydaje się funkcjonować prawidłowo, analiza odbieranego sygnału również nie wykazuje oznak fałszowania parametrów PNT, która w efekcie działającego oprogramowania malware nie jest prawidłowa.
- Fałszowanie poprawek różnicowych – fałszowany jest sygnał korekt przesyłanych w systemach różnicowych. Takie fałszowanie nie jest specjalnie niebezpieczne ponieważ korekty poprawiają pozycje odbiornika w zakresie 1-3m, a więc wpływ fałszywego sygnału korekt będzie również na poziomie 1-3m od prawidłowej pozycji.
- Fałszowanie sygnału konstelacji satelitów GPS – do fałszowania używa się generatora sygnału GPS dla pojedynczego satelity lub całej konstelacji. Efektem emisji fałszywego sygnału będzie „przykrycie" sygnału rzeczywistego, a zatem odbiornik będzie odbierał sygnał fałszywy uznając go za prawdziwy i na tej podstawie będzie wyznaczana pozycja. Ten właśnie typ fałszowania sygnału zostanie opisany szczegółowo.

Moc sygnału GPS na powierzchni ziemi wynosi średnio -130dBm [5]. Wiele odbiorników ma stosunkowo duży margines na dynamiczne zmiany poziomu sygnału. Jednocześnie powoduje to również większe możliwości fałszowania sygnału. Pomimo istnienia szeregu technik zmniejszania wpływu zakłócania na sygnał GNSS [6,7], nie są one powszechnie wykorzystywane przy produkcji urządzeń odbiorczych. Przeprowadzono szereg badań [8] dotyczących możliwości zakłócania odbiornika sygnałami generowanymi przez symulator konstelacji GPS. Okazało się, że przy pracującym na rzeczywistym sygnale odbiorniku, po wprowadzeniu zakłóceń z symulatora większych już o ok. 10 dB, odbiornik może przestać pracować stabilnie, aby po chwili przejąć fałszywe sygnały i podać użytkownikowi fałszywą pozycję. Im większa jest różnica w poziomach sygnałów (rzeczywisty – zakłócający), tym szybciej następuje proces przejęcia sfałszowanych danych. Warunkiem na skuteczne i niezauważalne dla użytkownika atakowanego odbiornika zakłócenie jest jednak konieczność przesyłania sygnałów dla satelitów widocznych tuż przed rozpoczęciem zakłócania. Nie jest więc możliwe sfałszowanie sygnału w taki sposób, aby odbiornik działający np. w Polsce miał pod wpływem ataku zacząć wskazywać pozycję np. w Australii.

Z punktu widzenia obrony systemu GPS przed przekłamaniami, fałszowanie jest bardziej skuteczne od zakłócania. W większości zastosowań, spoofing wymaga znacznie mniej energii, ponieważ korzysta z zysku przetwarzania sygnału GPS. Dla porównania, przy prostych zakłóceniach zagłuszających (jamming) do wytrącenia z pracy cywilnych

odbiorników (wykorzystujących emitowany przez satelity kod C/A) konieczne jest przewyższenie rzeczywistego sygnału o ok. 20-43dB. Dla odbiorników z kodem P różnica ta musi wynosić ok. 30-53dB. Jak już zostało wcześniej wspomniane, zakłócenia spoofing'owe mogą natomiast wpłynąć na pracę odbiornika przy sygnale fałszującym większym od sygnału rzeczywistego już o ok. 10dB. Spoofing w prostszej formie może spowodować brak możliwości nawigacji poprzez nasycenie odbiornika wiarygodnymi lecz fałszywymi sygnałami. Zaawansowane fałszowanie sygnału polega na tworzeniu fałszywych rozwiązań nawigacyjnych i ochronie tegoż fałszowania przed możliwością wykrycia przez użytkownika [9].

Ponieważ kod P jest silnie szyfrowany, jego fałszowanie jest znacznie utrudnione. Ogólnodostępny cywilny sygnał C/A jest natomiast stosunkowo łatwo podrobić, gdyż jego struktura, rodzaj modulacji i zasada rozpraszania widma są powszechnie znane, opisane w [5]. W dalszej części dokumentu przedstawiony zostanie opracowany w ITWL sposób generacji kodu C/A.

2. GENEROWANIE KODU C/A Z WYKORZYSTANIEM SPECJALIZOWANYCH MIKROPROCESORÓW

2.1 Słowo wstępu

Identyfikacja satelitów w systemie GPS oparta jest na metodzie podziału kodu CDMA (Code Division Multiple Access). Oznacza to, że wszystkie satelity emitują na tych samych częstotliwościach, ale sygnały modulowane są różnymi kodami. W dalszej części dokumentu analizie poddane zostaną zagadnienia związane tylko z kodem C/A. W celu identyfikacji konkretnego satelity należy przeprowadzić analizę otrzymanego ciągu bitów, ustalając którym fragmentem kodu odbierany sygnał został nacechowany (każdemu satelicie przypisany jest jeden konkretny fragment kodu) [10]. Warunkiem poprawnej identyfikacji satelitów przez odbiornik GPS jest wykrycie powtarzających się fragmentów kodów każdego z nich. W ramach przeprowadzonych badań, do implementacji algorytmu generacji kodu C/A wykorzystano układy programowalne rodziny FPGA.

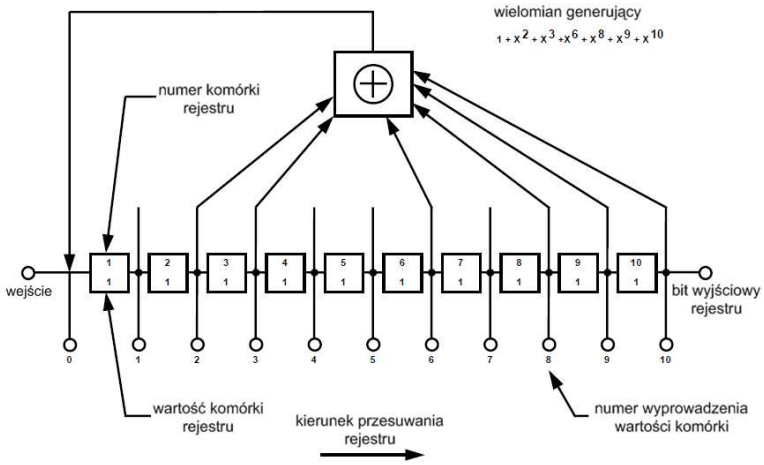
2.2 Opis algorytmu generowania kodu C/A

Kolejne bity kodu C/A generowane są przez dokonywanie operacji XOR na wartościach opuszczających dwa rejestry przesuwne LFSR (Linear Feedback Shift Register): G1 i G2. Każdy z nich składa się z 10 komórek, zaś na okresy obu składają się 1023 takty. Uzależnienie kodu od numeru satelity dokonywane jest przez wstrzymanie reinicjacji rejestru G2 na określoną liczbę taktów. Rejestry taktowane są z częstotliwością 1.023 MHz, i posiadają ten sam wektor inicjujący o wartości 1111111111. Wielomiany generujące dla G1 i G2 przyjmują postać:

G1: 1+X10+X3

G2: 1+X2+X3+X6+X8+X9+X10

Rysunek nr 1 prezentuje schemat budowy rejestru G2. Analogicznie wygląda schemat dla rejestru G1.



Rys. 1. Schemat budowy rejestru przesuwnego G2

Wstrzymanie reinicjacji rejestru G2 związane z uzależnieniem kodu od numeru satelity może zostać zastąpione dokonaniem operacji XOR dwóch wartości ściśle określonych komórek rejestru. Zabieg ten umożliwia jednak wygenerowanie jedynie ograniczonej liczby poprawnych ciągów kodowych. Numery komórek rejestrów, na podstawie których można uzyskać wyniki równoważne wprowadzeniu danej wartości przesunięcia przedstawia tabela 1.

Tab. 1. Wektory testowe dla kodów C/A i P przy kolejnych przesunięciach (z zakresu 1~19)

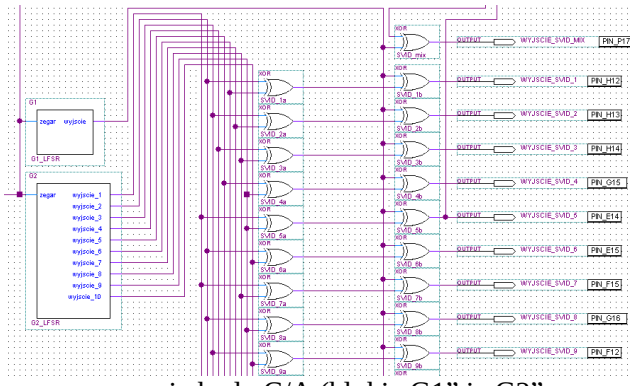
Przesunięcia i wektory testowe kodów poszczególnych satelitów							
nr SV ID	nr sygnału GPS PRN	przesunięcia fazowe kodów		opóźnienia kodów (takty)		pierwsze 10 bitów kodu C/A (oktalnie)	pierwsze 12 bitów kodu P (oktalnie)
		C/A($G2_j$)****	($X2_i$)	C/A	P		
1	1	2 ⊕ 6	1	5	1	1440	4444
2	2	3 ⊕ 7	2	6	2	1620	4000
3	3	4 ⊕ 8	3	7	3	1710	4222
4	4	5 ⊕ 9	4	8	4	1744	4333
5	5	1 ⊕ 9	5	17	5	1133	4377
6	6	2 ⊕ 10	6	18	6	1455	4355
7	7	1 ⊕ 8	7	139	7	1131	4344
8	8	2 ⊕ 9	8	140	8	1454	4340
9	9	3 ⊕ 10	9	141	9	1626	4342
10	10	2 ⊕ 3	10	251	10	1504	4343
11	11	3 ⊕ 4	11	252	11	1642	|
12	12	5 ⊕ 6	12	254	12	1750	|
13	13	6 ⊕ 7	13	255	13	1764	|
14	14	7 ⊕ 8	14	256	14	1772	|
15	15	8 ⊕ 9	15	257	15	1775	|
16	16	9 ⊕ 10	16	258	16	1776	|
17	17	1 ⊕ 4	17	469	17	1156	|
18	18	2 ⊕ 5	18	470	18	1467	|
19	19	3 ⊕ 6	19	471	19	1633	4343

SVID - Space Vehicle Identification
PRN - Pseudo Random Noise

Analizując wyżej zamieszczoną tabelę można na przykład stwierdzić, że 7-bitowemu przesunięciu kodu odpowiada XOR-owanie 1 i 8 bitu rejestru G2 (wiersz oznaczony czerwoną ramką). Zabieg ten pozwala znacznie uprościć implementację algorytmu. Aby uzyskać wynikowy bit kodu C/A należy więc obliczyć wynik operacji XOR na dwóch bitach G2 i bicie opuszczającym rejestr G1.

2.3 Implementacja algorytmu

Algorytm został zaimplementowany z wykorzystaniem struktury hierarchicznej. Połączenia konkretnych komórek rejestrów (w zależności od numeru satelity) są widoczne na schemacie algorytmu (rysunek 2) jako kolumny bramek XOR. Obydwa rejestry zostały natomiast zaimplementowane jako osobne bloki.

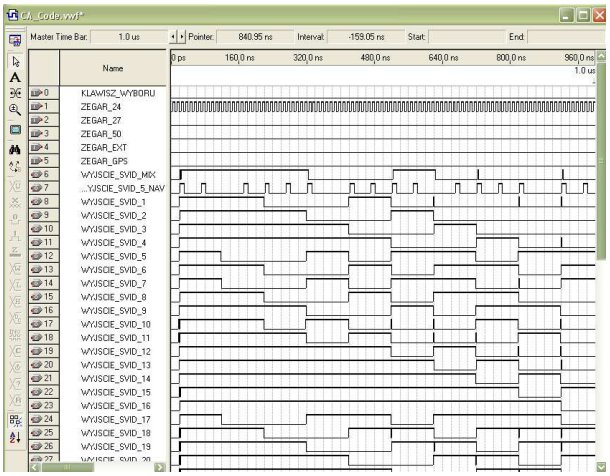


Rys. 2. Schemat algorytmu generowania kodu C/A (bloki „G1" i „G2" oraz zestaw bramek XOR)

Na schemacie można także zauważyć „podpięcie" konkretnych wyjść (pinów) układu do wyjść konkretnych bramek prawej kolumny. Jest to „fizyczne" połączenie schematu z rzeczywistym układem. Rysunek 2 przedstawia tylko część schematu (dla satelitów od 1 do 9). Analogicznie wykonane zostały połączenia bramek dla pozostałych satelitów. W układzie zaimplementowano także osobne wyjście („WYJSCIE_SVID_MIX"), na które podawane są naprzemiennie kody dla kilku satelitów naraz (np. 1023 bitów kodu dla pierwszego, 1023 dla drugiego i znów 1023 bitów dla pierwszego). Takie rozwiązanie przyjęto z myślą o prowadzeniu badań nad możliwościami odbiorczymi odbiorników (czy uda się symulować kilka satelitów na jednym kanale, jeśli tak to ile, i po ile bitów kodu minimalnie można wysyłać dla każdego z nich). Implementacja funkcji przeplatającej sygnały z kilku satelitów (do dwunastu) zawarta jest w niewidocznym na zamieszczonym wyżej rysunku bloku. Na wejście zegarowe wszystkich bloków doprowadzany jest sygnał z zewnętrznego oscylatora kwarcowego 10.23 MHz (osobny układ, pobierający z płytki jedynie zasilanie).

2.4 Sprawdzenie poprawności otrzymywanych kodów

Zaimplementowany algorytm generacji kodu C/A został przetestowany z wykorzystaniem narzędzia symulacji będącego częścią użytego środowiska programistycznego. Symulacja działania programu odbywa się przez wprowadzenie wektorów testowych, uruchomienie symulacji i obserwację zmian stanów sygnałów na śledzonych wyjściach układu. Wynik działania symulacji przedstawia rysunek 3.



Rys. 3. Wynik symulacji działania układu

Użyty w symulacji sygnał zegarowy nie posiadał częstotliwości generowania kodu C/A 10.23 MHz, lecz nie ma to wpływu na ocenę poprawności układu. Po krótkiej obserwacji

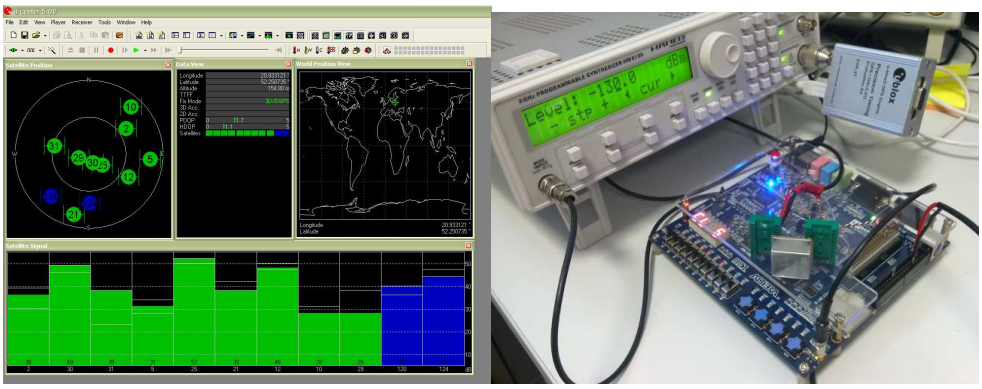
przebiegów czasowych można zauważyć, że pokrywają się one z wektorami testowymi zapisanymi w specyfikacji algorytmu [5]. I tak na przykład dla satelity nr 6, pierwsze 10 bitów zapisanych ósemkowo daje ciąg 1455, co pokrywa się z wartością podaną w tabeli nr 1. Należy jednak pamiętać, że zawsze pierwszy sygnał wysoki na przebiegach czasowych musi być już interpretowany jako pierwsza trójka bitów (001), z czego przebieg zaczyna się dopiero od wartości 1.

3. SYMULACJA SYGNAŁÓW IDENTYFIKACYJNYCH POSZCZEGÓLNYCH SATELITÓW

3.1 Wprowadzenie

Zarówno kod P jak i C/A transmitowany jest z użyciem częstotliwości nośnej (1575.42 MHz dla C/A i 1227.6 MHz dla P). Częstotliwość nośna jest modulowana pojawiającymi się kolejnymi bitami kodu z użyciem modulacji BPSK (szczegóły w [11]). Po uzyskaniu ciągu kodowego kolejnym etapem jest więc wytworzenie fali nośnej i jej modulacja. Użyty na potrzeby badań generator umożliwia generowanie sygnałów o częstotliwościach od 1 Hz do 3GHz. Posiada także wbudowany modulator BPSK oraz wewnętrzny programowalny tłumik. Moc wyjściowego sygnału może być regulowana w zakresie między -135 a 13 dBm.

Aby sprawdzić, czy nadawany przez generator i zmodulowany ciągiem produkowanym przez układ FPGA sygnał umożliwia jednoznaczne określenie satelity któremu miał być przyporządkowany, należało podać go na odbiornik GPS. Dołączone do wykorzystanego w badaniach odbiornika oprogramowanie pozwala między innymi na określenie pozycji odbiornika na ziemi, satelitów na horyzoncie, oraz poziomów stosunku sygnał/szum od poszczególnych satelitów. Przykładowy zrzut ekranu z działania oprogramowania odbiornika (rzeczywisty sygnał odbierany w Warszawie) przedstawia rysunek 4 (po lewej).



Rys. 4. Zobrazowanie pracy oprogramowania odbiornika (po lewej) i zestaw pomiarowy wykorzystywany do badania możliwości symulowania sygnałów satelitów (po prawej)

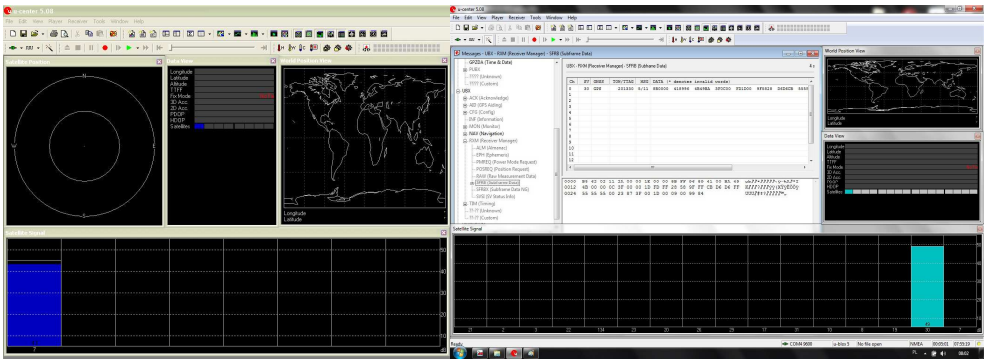
Z obserwacji zobrazowania wynika, że odbierane i wykorzystywane do obliczeń pozycji są satelity nr: 2, 30, 31, 5, 25, 21, 12, 10 i 29 (kolor zielony). Satelity nr 120 i 124 to satelity przesyłające wyłącznie dane korekcyjne a ich kody nie zostają wykorzystane do obliczenia pozycji (kolor niebieski).

3.2 Symulacja sygnału identyfikacyjnego pojedynczego satelity z użyciem jednego kanału

W przypadku, gdy do odbiornika podłączony zostanie generator modulowany kodem C/A, w oknie „Satellite Signal” powinien się pojawić tylko jeden słupek, przyporządkowany

satelicie o numerze określonym przez pin, z którego pobierany będzie sygnał modulujący (kod dla każdego satelity wyprowadzany jest z płytki ewaluacyjnej na oddzielnym pinie). Zestaw pomiarowy: generator, płytka ewaluacyjna, zewnętrzny oscylator 10.23 MHz oraz podłączony do komputera odbiornik GPS zaprezentowany został na rysunku nr 4 (po prawej). W zestawie tym zewnętrzny oscylator 10.23 MHz wystawia sygnał zegarowy na wejście układu. Tłumienie wewnętrzne generatora ustawione zostało na -130 dBm.

Po uaktywnieniu wyjścia generatora sygnał podawany jest na odbiornik, i zgodnie z oczekiwaniami oprogramowanie wykrywa tylko jednego satelitę o numerze identyfikacyjnym SVID równym 7 (rysunek 5 - okno po lewej).

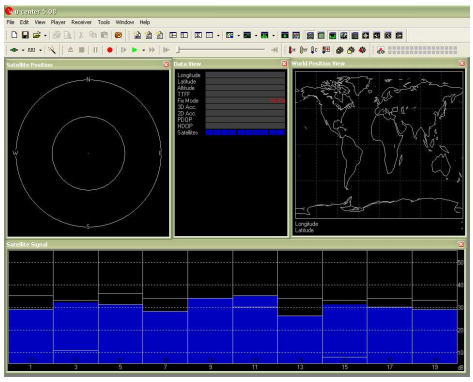


Rys. 5. Aplikacja odbierająca symulowane sygnały satelitów: nr 7 (z lewej) i nr 30 z dołączoną depeszą nawigacyjną (z prawej).

Po przełączeniu sygnału modulującego na wyprowadzenie odpowiadające innemu symulowanemu satelicie, na ekranie wykryty zostaje tenże satelita. W wyniku przeprowadzonych prac zaimplementowano także algorytm generowania wiadomości nawigacyjnej. Wiadomość ta jest przesyłana razem z kodem C/A satelity i „informuje" odbiornik m.in. na temat aktualnych parametrów orbit, czy poprawek koniecznych do uwzględnienia podczas obliczeń. Okno aplikacji odbiornika, na którego wejście podany został sygnał z dołączoną wiadomością widoczny jest na rysunku 5 (okno po prawej). Poprawność odbioru depeszy sygnalizuje turkusowy kolor używany przy prezentacji danych konkretnego satelity.

3.3 Symulacja sygnałów identyfikacyjnych kilku satelitów z użyciem jednego kanału

Jak już wcześniej zostało wspomniane, zastosowany układ umożliwiał także przesyłanie naprzemiennie kodów kilku satelitów na jednym kanale. W trakcie prowadzonych badań pozostawał do rozwiązania problem jaka jest maksymalna liczba satelitów możliwa do symulacji (aby sygnał żadnego z nich nie zanikał), oraz jak długi ciąg bitów kodu dla jednego satelity wystarczy do poprawnego zidentyfikowania go przez odbiornik. Na potrzeby tego opracowania zaprogramowano układ tak, aby symulował na jednym kanale 10 pierwszych satelitów o nieparzystych numerach (1,3,5,7 itp.). Wyniki widoczne są na rysunku 6.

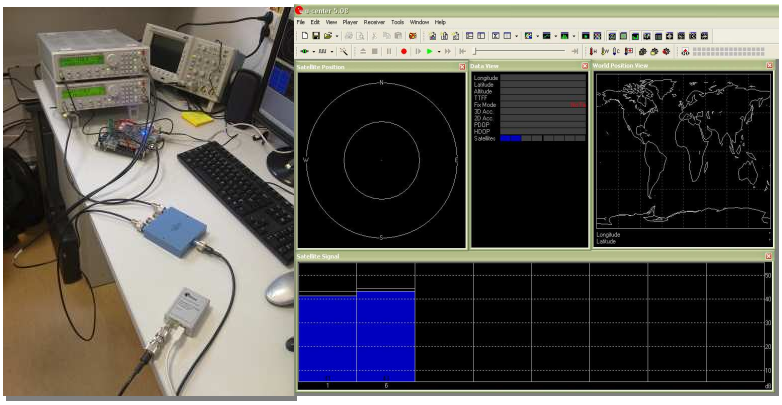


Rys. 6. Symulowanie sygnału nadawanego przez 10 pierwszych satelitów o nieparzystych numerach.

Można zauważyć, że sygnały (stosunek sygnał/szum) wszystkich satelitów różnią się między sobą poziomami mocy (odwzorowanymi przez wysokości słupków w dolnej części okna). Poziomy te zmieniają się, czasem do tego stopnia, że sygnał może na chwilę całkowicie zaniknąć. Dzieje się tak, gdyż jeden kanał jest współdzielony między 10 różnymi sygnałami. Aby sygnały były widoczne, konieczne było także zmniejszenie tłumienia generatora z -130 dBm do -115 dBm.

3.4 Symulacja sygnałów identyfikacyjnych kilku satelitów z użyciem dwóch kanałów

W ramach badań, przeprowadzono także próby symulacji satelitów z dwóch niezależnych od siebie kanałów (dwa generatory). Modulowane sygnały z każdego z nich sumowane były na sumatorze a następnie podawane na wejście odbiornika. Zestaw symulujący przedstawiono na rysunku 7 (po lewej).



Rys. 7. Po lewej: zestaw symulujący sygnały dwóch satelitów (dwa osobne kanały), po prawej: sygnały satelitów odebrane na odbiorniku (satelity nr 1 i 6).

Modulacja częstotliwości nośnej wykonywana była z zastosowaniem kodów satelitów nr 1 i 6. Okno aplikacji odbiornika prezentujące wyniki otrzymane po włączeniu urządzeń zostało przedstawione na rysunku 7 (prawa część). Dla celów testowych sprawdzono także pozostałe konfiguracje sygnałów. Za każdym razem otrzymywane wyniki były zgodne z oczekiwaniami. Należy zauważyć, że dla opcji generowania sygnałów z dwóch niezależnych kanałów (dwa generatory) fluktuacje stosunku sygnał/szum odbieranych sygnałów są nieznaczne, w przeciwieństwie do przypadku, gdy sygnały generowane dla kilku satelitów przesyłane były naprzemiennie z użyciem tylko jednego kanału. Przy wykorzystaniu techniki

naprzemiennego nadawania kodów kilku satelitów jednocześnie w każdym z dwóch kanałów, przy użyciu opisywanego zestawu możliwe jest nadawanie do 24 sygnałów naraz.

PODSUMOWANIE

Spoofing będąc bardziej wyrafinowaną, „inteligentną" metodą wprowadzania zakłóceń pracy odbiorników systemu GPS jest jednak znacznie trudniejszy do przeprowadzenia niż proste zagłuszanie (jamming). Cała trudność polega na konieczności zastosowania złożonego urządzenia mogącego imitować sygnały kilku (min. czterech) satelitów jednocześnie. Kompletne rozwiązania (emulatory konstelacji widocznych satelitów) gwarantują skuteczność przeprowadzenia ataku przekłamującego wskazania odbiornika o odległość rzędu kilkuset metrów do kilku kilometrów. Przeprowadzone w ITWL badania potwierdziły możliwość wprowadzenia zakłóceń w pracę systemów wykorzystujących nawigację satelitarną, zwłaszcza przy stosowaniu kodu C/A. W pełni satysfakcjonujący zestaw spooging'owy nie jest co prawda urządzeniem tanim i prostym, ale należy liczyć się z możliwością jego zastosowania. Wszędzie tam, gdzie brak orientacji nawigacyjnej może być przyczyną powstania zagrożeń zwłaszcza dla życia ludzkiego, należy powyższą ewentualność brać pod uwagę i stosować rozwiązania wspomagające w określaniu wartości parametrów PNT.

ANALYSIS OF THE POSSIBILITIES OF PERFORMING A SPOOFING ATTACK – THE INTENTIONAL WAY OF AFFECTING THE GPS SATELLITE NAVIGATION SYSTEM RECEIVER'S FUNCTIONING

Abstract

This paper presents the results of the research carried out in ITWL, concerning the possibility of generating signals emitted by the GPS Satellite Navigation System satellites. It is possible to perform a spoofing attack on the receiver, if it is able to receive at least 4 properly prepared signals. The methods of generating these single and multichannel satellite signals (using one or more generators) will be discussed.

BIBLIOGRAFIA

1. J.A. Volpe: *Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System, Technical report,* National Transportation Systems Center, 2001
2. Praca zbiorowa*: Wpływ spoofing'u na poprawność określania pozycji przez odbiornik GPS,* ITWL 2010
3. M. Tanase: *IP Spoofing: An Introduction,* Symantec Security Blog, 2003
4. A. Lockhart: *Network Security Hacks*, O'Reilly, 2007
5. Praca zbiorowa: *Navstar GPS Space Segment/Navigation User Interfaces (ICD-GPS-200C with IRN-200C-004),* U.S. Government Printing Office, 2000
6. E.D. Kaplan, P. Ward: *Understanding GPS: principles and applications,* str. 209-236, Artech House, 1996
7. B.W. Parkinson, J.J. Spilker, B.D. Elrod: *Global positioning system: theory and applications*, str. 51-79, JR American Institute of Aeronautics and Astronautics, 1996

8. Praca zbiorowa: *Opracowanie technologii zagłuszania i przeciwdziałania celowym zakłóceniom systemów nawigacji satelitarnej GNSS*, ITWL 2011
9. J.S. Warner, R.G. Johnson: *GPS Spoofing Countermeasures*, Homeland Security Journal, 2003
10. Praca zbiorowa: *GPS Essentials of Satellite Navigation Compendium*, u-blox AG, 2009
11. P. Kowaleczko, J. Sulkowski: *Podatność systemu nawigacji satelitarnej GPS na zakłócenia i wynikające z niej zagrożenia dla transportu*, Logistyka, nr 3/2012

Autorzy:
mgr inż. Piotr KOWALECZKO – Instytut Techniczny Wojsk Lotniczych
dr inż. Jarosław SULKOWSKI– Instytut Techniczny Wojsk Lotniczych