Biuletyn WAT
Vol. LXII, Nr 4, 2013

Demonstrator programowalnej stacji zakłóceń

KRZYSZTOF MALON, JERZY ŁOPATKA

Wojskowa Akademia Techniczna, Wydział Elektroniki, Instytut Telekomunikacji,
00-908 Warszawa, ul. gen. S. Kaliskiego 2,
kmalon@wat.edu.pl, jlopatka@wat.edu.pl

Streszczenie. Na obecnym polu walki elektronicznej bardzo ważnym zagadnieniem jest poszukiwanie coraz bardziej skutecznych i efektywnych metod kontroli łączności radiowej przeciwnika. Jednym z istotnych punktów związanych z tą tematyką jest zakłócanie łączności, które może być również wykorzystane jako ochrona przed improwizowanymi ładunkami wybuchowymi IED (ang. *Improvised Explosive Device*). Jako docelowe miejsce montażu stacji zakłóceń mających na celu zabezpieczenie przed powyższymi zagrożeniami stosuje się typowe pojazdy wojskowe lub bezzałogowe platformy lądowe UGV (ang. *Unmanned Grodnu Vehicle*).
W artykule przedstawione zostały podstawowe techniki zakłócania z uwzględnieniem cech i właściwości wskazujących na zakres ich stosowania. Następnie opisano stanowisko laboratoryjne do badania skuteczności zakłóceń wybranych systemów oraz wskazano metodykę doboru optymalnych parametrów sygnału zakłócającego. Celem optymalizacji powyższych parametrów była minimalizacja energii sygnału zakłócającego. Zaprezentowane stanowisko posłużyło także do przeprowadzenia testów zakłócania synchronicznego, wyzwalanego każdym odbieranym pakietem danych. Dalszą część referatu stanowi charakterystyka demonstracyjnej wersji stacji zakłóceń. W tym przypadku zastosowano zakłócanie asynchroniczne z wykorzystaniem przygotowanego waveformu. Jako przykład możliwości działania stacji przedstawiono jeden z trybów jej pracy podczas realizacji zadania odzewowego.
Słowa kluczowe: telekomunikacja, walka elektroniczna, zakłócanie, improwizowane ładunki wybuchowe

1. Wstęp

Próby zakłócania transmisji radiowych pojawiły się niedługo po powstaniu samej radiokomunikacji. Jest to zjawisko, które towarzyszy rozwojowi technik przesyłania informacji drogą radiową i w związku z tym metody i sposoby zakłócania podlegają również ciągłym modyfikacjom i ulepszeniom.

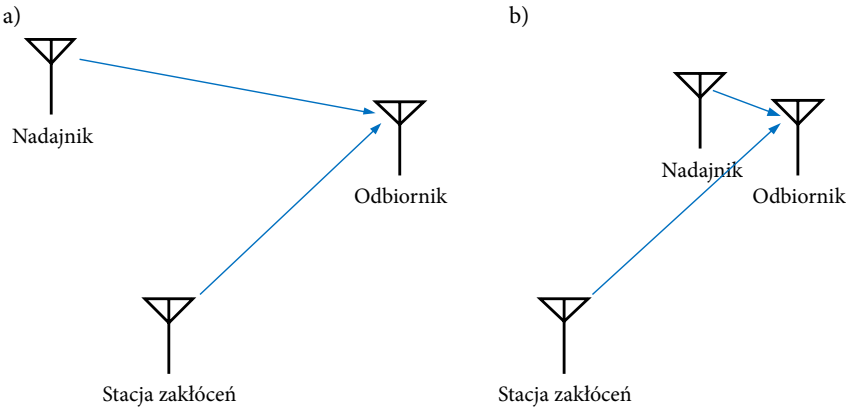
Jak pisze autor [1], w świadomości ludzi utrwaliły się pewne błędne pojęcia dotyczące zakłócania. Pierwszym z nich jest koncepcja „zakłócania transmisji". Jest to możliwe w teorii, lecz w większości przypadków wyróżnia się odbiornik, który powinien być zakłócony. Stanowi on miejsce w systemie, w którym sygnał jest najsłabszy, a przez to najbardziej podatny na zakłócenia. W miejscu odbiornika moc sygnału pochodząca od urządzenia zakłócającego powinna przewyższać moc docierającą od nadajnika. Współczynnik wymagany do efektywnego zakłócania oznaczany jako J/S (ang. *Jamming to Signal ratio*) określa stosunek mocy sygnału zakłócającego (J) do mocy sygnału zakłócanego (S) i wyrażany jest zazwyczaj w dB (rys. 1a). Według [2] wzór na określenie powyższego parametru składa się z następujących elementów:

$$J / S = ERP_J - ERP_S - L_J + L_S + G_{RJ} - G_R, \tag{1}$$

gdzie: J/S — stosunek mocy sygnału zakłócającego do mocy sygnału zakłócanego na wejściu odbiornika (w dB);
ERP_J — efektywna moc wypromieniowana przez urządzenie zakłócające (w dBm);
ERP_S — efektywna moc wypromieniowana przez nadajnik (w dBm);
L_J — straty propagacji od urządzenia zakłócającego do odbiornika (w dB);
L_S — straty propagacji od nadajnika do odbiornika (w dB);
G_{RJ} — zysk anteny odbiorczej w kierunku urządzenia zakłócającego (w dBi);
G_R — zysk anteny odbiorczej w kierunku nadajnika (w dBi).

Drugim często popełnianym błędem jest przekonanie, że zakłócanie jest bezwzględne (absolutne, całkowite) i zapobiega przed odbiorem sygnału w każdym przypadku. Jest to również stwierdzenie nie zawsze znajdujące odzwierciedlenie w praktyce, gdyż należy pamiętać o koncepcji zwanej *burn-through*, która dotyczy wymaganej odporności łącza potrzebnej, aby zniwelować efekt zakłócania. W przypadku istnienia wystarczająco silnego łącza pomiędzy nadajnikiem i odbiornikiem, stacja zakłóceń nie jest w stanie zablokować komunikacji między nimi (rys. 1b).

Podczas zakłócania sygnałów analogowych konieczne jest zwykle osiągnięcie wysokich wartości współczynnika J/S (dla większości modulacji wartość 10 dB uważana jest za wystarczającą). Dodatkowo w większości przypadków należy generować zakłócenia w trybie ciągłym (współczynnik wypełnienia sygnału zakłócającego równy 1). Natomiast w sytuacji zakłócania sygnałów cyfrowych, którego celem jest uniemożliwienie odczytu informacji przez demodulator, poprzez m.in. dążenie do zerwania synchronizacji, możliwe jest zmniejszenie współczynnika wypełnienia sygnału zakłócającego do 1/3 [2].



Rys. 1. Rozmieszczenie elementów w zakłócanym systemie [1]: a) podstawowy scenariusz; b) efekt *burn-through*

2. Techniki zakłócania

Jak wspomniano na wstępie artykułu, wraz z rozwojem radiokomunikacji pojawiają się coraz bardziej wyszukane metody zakłócania. Urządzenie zakłócające może wykorzystywać różne możliwe strategie działania, gdyż każda technika charakteryzuje się pewnymi zaletami i wadami, które wskazują rozwiązanie najlepsze dla konkretnego zastosowania. Przykładowa klasyfikacja technik zakłócania wg [3] wyróżnia zakłócanie:

- szumowe (ang. *noise jamming*),
  - szerokopasmowe (ang. *broad band*, *full band*, *barrage jamming*),
  - części pasma (ang. *partial band*),
  - wąskopasmowe (ang. *narrow band*),
- nośną, tonem (ang. *tone jamming*),
  - pojedynczym tonem (ang. *single tone*, *spot jamming*),
  - wieloma tonami (ang. *multiple tones*, *comb jamming*),
- przestrajane (ang. *swept jamming*),
- impulsowe (ang. *pulse jamming*),
- odzewowe (ang. *follower jamming*, *responsive jamming*, *repeater jamming*),
  - z szumem wąskopasmowym (ang. *follower jamming with narrow band noise*),
  - z nośną (ang. *follower tone jamming*),
- inteligentne (ang. *smart jamming*).

Dwie pierwsze kategorie zakłócania szumowego polegają na wygenerowaniu sygnału w części lub w całym paśmie systemu zakłócanego, przy czym sygnał ten nie zmienia swojego położenia na widmie. Szum wąskopasmowy wykorzystywany może być w połączeniu z zakłócaniem odzewowym, w którym próbuje się nadążać za zmianami częstotliwości np. w systemach FH (ang. *Frequency Hopping*). W takiej

sytuacji system zakłócający musi być wyposażony w elementy skanujące wybrane zakresy pasma oraz spełniać wymagania czasowe wynikające z trybu pracy systemu zakłócanego. Zakłócanie wieloma nośnymi polega na odpowiednim ich rozmieszczeniu na widmie i może być stosowane przeciwko systemom DSSS (ang. *Direct Sequence Spread Spectrum*) i FHSS (ang. *Frequency Hopping Spread Spectrum*). Koncepcją umożliwiającą zakłócanie szerokopasmowe jest zastosowanie sygnału przestrajanego, który zmienia swoją częstotliwość w zadanych zakresach i w określonym czasie. Innym rozwiązaniem może być wytwarzanie krótkich impulsów powodujące uzyskiwanie szerokiego pasma w momencie ich generacji. Najbardziej zaawansowanym sposobem zakłócania jest stosowanie inteligentnych technik, które działają na określone fragmenty sygnału zakłócanego. Niestety wymaga to posiadania dokładnej wiedzy na temat zakłócanych sygnałów oraz wymusza uzyskanie synchronizacji. Oprócz wymienionych powyżej metod zakłócania wyróżnia się także zakłócanie dezinformujące polegające na wysyłaniu do odbiornika fałszywych wiadomości.

3. Sformułowanie funkcji celu

Celem doboru optymalnych parametrów sygnału zakłócającego była minimalizacja energii zakłóceń przy zachowaniu skuteczności działania. Zakładając stały, wystarczający do uzyskania wymaganej wartości współczynnika J/S, poziom mocy sygnału zakłócającego, optymalizowanym parametrem był całkowity czas generacji zakłóceń. W związku z tym sformułowano następującą funkcję podlegającą minimalizacji:

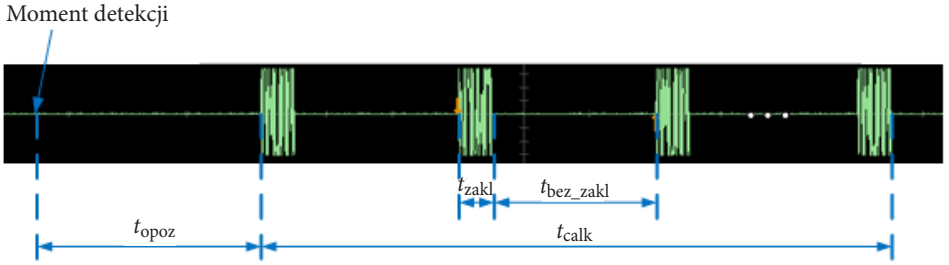
$$f(t_{\text{zakl}}, t_{\text{calk}}, t_{\text{bez\_zakl}}, t_{\text{opoz}}) = t_{\text{zakl}} + t_{\text{calk}} - t_{\text{bez\_zakl}} - t_{\text{opoz}} \rightarrow \min, \tag{2}$$

gdzie: t_{zakl} — czas generacji pojedynczego impulsu zakłóceń → min;
t_{calk} — czas mierzony od momentu rozpoczęcia zakłócania celu do zakończenia → min;
t_{opoz} — czas od wykrycia sygnału celu do rozpoczęcia jego zakłócania → max;
$t_{\text{bez\_zakl}}$ — czas przerwy w zakłócaniu pomiędzy kolejnymi impulsami zakłócającymi → max.

Wszystkie powyższe parametry muszą spełniać następujące ograniczenia:

$$t_{\text{zakl}}, t_{\text{bez\_zakl}}, t_{\text{opoz}}, t_{\text{calk}} \geq 0. \tag{3}$$

Na rysunku 2 przedstawiono charakterystyczne przedziały czasowe istotne z punktu widzenia optymalizacji oraz zależności między nimi.



Rys. 2. Charakterystyczne czasy podlegające optymalizacji

Na podstawie wymienionych parametrów czasowych wyróżnić można dodatkowo współczynnik wypełnienia sygnału zakłócającego wyrażony poniższym wzorem:

$$k = \frac{t_{zakl}}{t_{zakl} + t_{bez\_zakl}} = \frac{t_{zakl}}{t_{okres}} \rightarrow \min, \tag{4}$$

gdzie: k — współczynnik wypełnienia sygnału zakłócającego;
t_{okres} — okres powtarzania impulsów zakłócających.

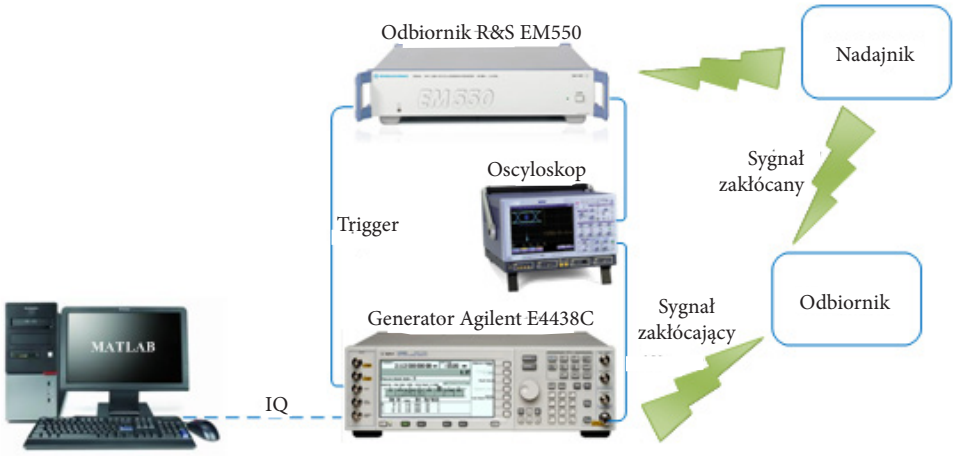
$$t_{okres} = t_{zakl} + t_{bez\_zakl} \rightarrow \max. \tag{5}$$

Maksymalizacja czasów t_{bez_zakl} i t_{opoz} wynikająca z minimalizowania energii sygnału zakłócającego jest również celowa z punktu widzenia możliwości wykorzystania odstępów między impulsami do monitorowania widma (poszukiwania nowych celów bądź podjęcia decyzji o zakończeniu zakłócania aktualnego celu) lub zakłócania innych celów.

4. Stanowisko laboratoryjne do badania skuteczności zakłóceń wybranych systemów — zakłócanie synchroniczne

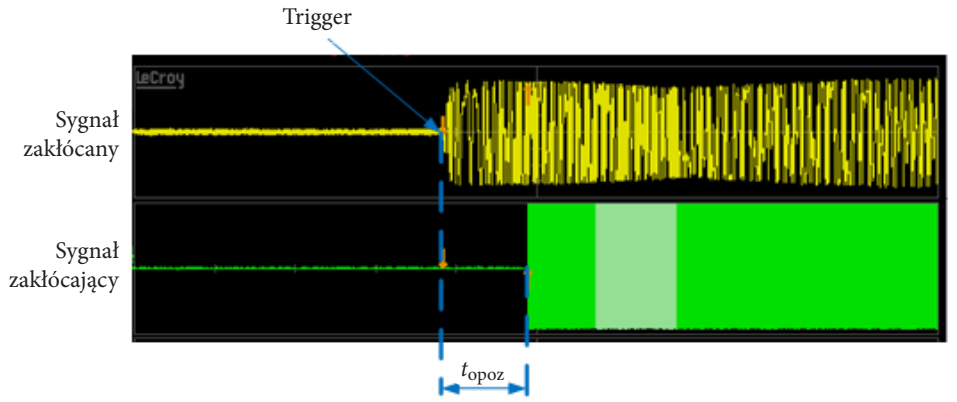
W celu testowania skuteczności zakłóceń wybranych systemów zestawiono stanowisko laboratoryjne przedstawione na rysunku 3. Składa się ono z: odbiornika R&S EM550 pełniącego rolę detektora energii pracującego na stałej częstotliwości, generatora sygnałów arbitralnych Agilent E4438C generującego zakłócenia o zadanej strukturze i czasie trwania (struktura sygnału zakłócającego tworzona była w środowisku MATLAB i w postaci próbek IQ wgrywana do pamięci generatora) oraz oscyloskopu służącego do pomiaru charakterystycznych przedziałów czasowych. Oprócz wymienionych urządzeń laboratoryjnych wykorzystano także nadajniki i odbiorniki następujących systemów:

— GSM (ang. *Global System for Mobile Communications*),
— radiotelefony PMR (ang. *Private Mobile Radio*),
— zdalne otwieranie bramy garażowej,
— telefonia satelitarna.



Rys. 3. Stanowisko laboratoryjne do badania skuteczności zakłóceń wybranych systemów

Pierwszym parametrem podlegającym optymalizacji był czas opóźnienia generacji sygnału zakłócającego od momentu detekcji sygnału celu. Przykładowy pomiar wykonany za pomocą oscyloskopu przedstawiono na rysunku 4. Wykorzystano w tym celu bezpośrednie połączenie wyjścia VIDEO (składowe I lub Q) odbiornika z wejściem PATT TRIG IN generatora oraz opcję wprowadzania dodatkowego

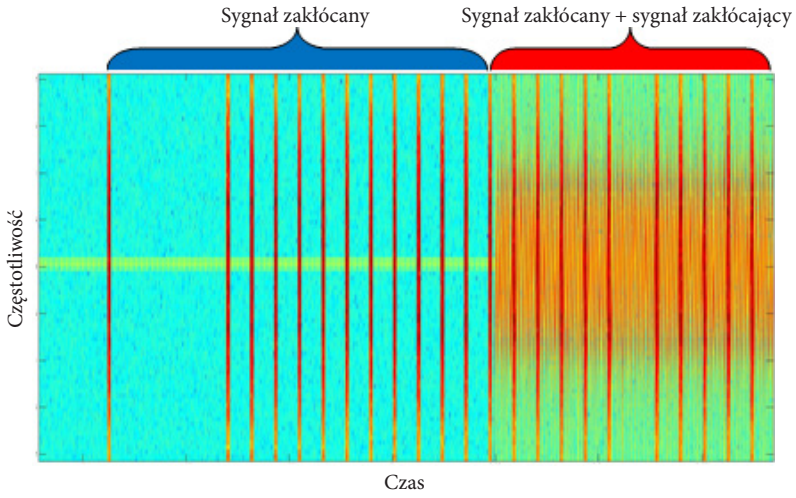


t_{opoz} – czas od wykrycia sygnału celu do rozpoczęcia jego zakłócania

Rys. 4. Pomiar maksymalnego czasu opóźnienia generacji sygnału zakłócającego w trybie ciągłym

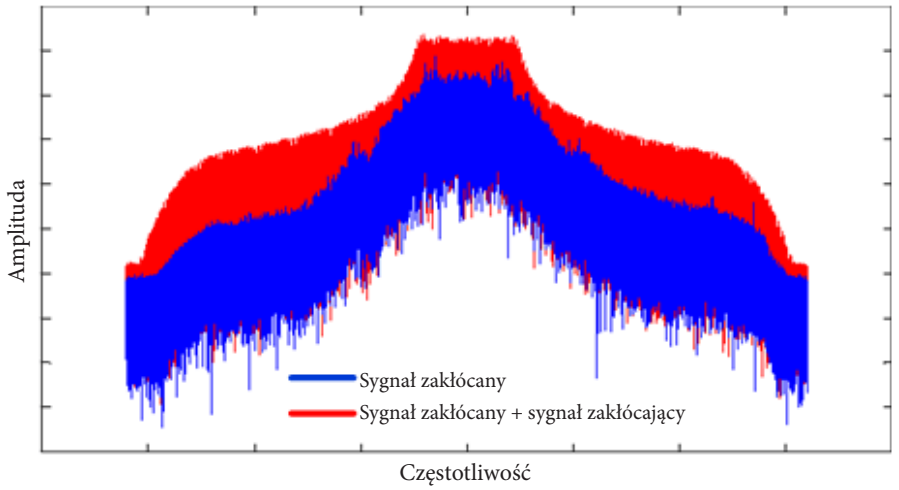
opóźnienia w generatorze Agilent (rys. 3). W tym przypadku zastosowano zakłócanie w trybie ciągłym polegające na generacji sygnału zakłócającego o współczynniku wypełnienia równym 1.

W celu dokładniejszej analizy zależności pomiędzy sygnałem zakłócanym a zakłócającym skorzystano także z możliwości rejestracji próbek IQ poprzez interfejs LAN (ang. *Local Area Network*) odbiornika EM550 R&S. Sygnały po zapisie na dysk komputera oraz odpowiedniej obróbce w środowisku MATLAB były analizowane za pomocą spektrogramu (rys. 5) ukazującego relacje czasowe oraz strukturę częstotliwościową sygnałów. Dodatkowo na rysunku 6 przedstawiono możliwość porównywania widm amplitudowych sygnałów zakłócanych i zakłócających.

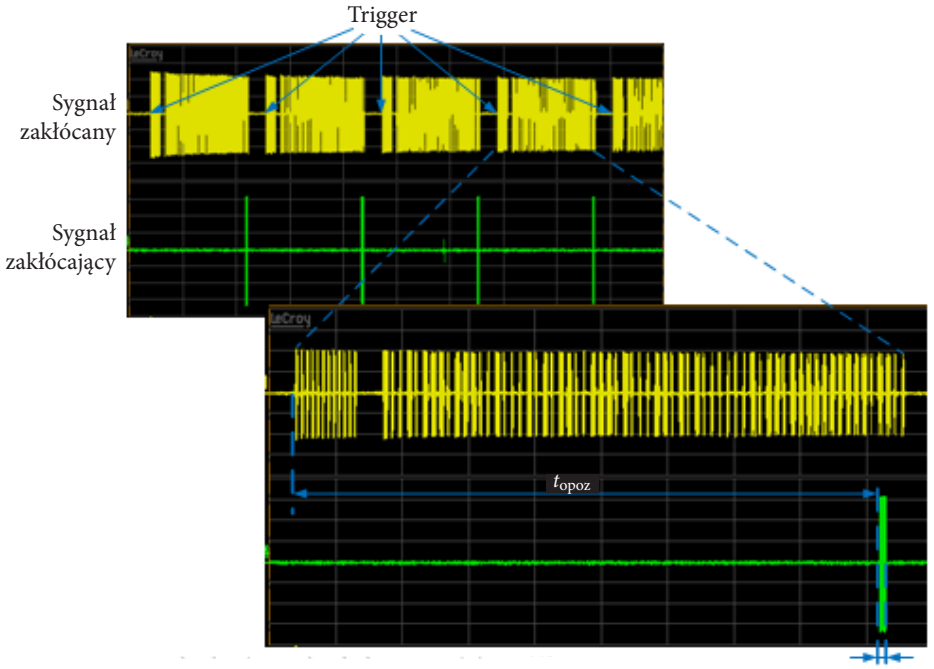


Rys. 5. Spektrogram sygnału zakłócanego i zakłócającego

Kolejne parametry podlegające optymalizacji testowane były w trybie zakłócania synchronicznego. Idea tego typu zakłóceń polega na generacji impulsów zakłócających wyzwalanych kolejnymi pakietami danych. Dzięki takiemu podejściu uzyskuje się zsynchronizowanie zakłóceń z sygnałem danego systemu, co umożliwia zakłócanie poszczególnych części sygnału charakterystyczne dla metody inteligentnego zakłócania. W przypadku transmisji pakietowych (cyfrowych), np. sygnału do otwierania bramy garażowej (rys. 7), istotnymi parametrami są: czas opóźnienia generacji sygnału zakłócającego oraz czas jego trwania. Za pomocą zmiany czasu t_{opoz}, który z punktu widzenia kryterium optymalizacji przedstawionego w punkcie 3 powinien być maksymalny, możliwe jest poszukiwanie najbardziej wrażliwych na zakłócenia części pakietów. Ograniczeniem występującym przy analizie tego parametru jest opóźnienie wprowadzane przez system detekcyjno-zakłócający, które wynosiło w tym przypadku poniżej 100 μs. Zastosowanie tej samej techniki



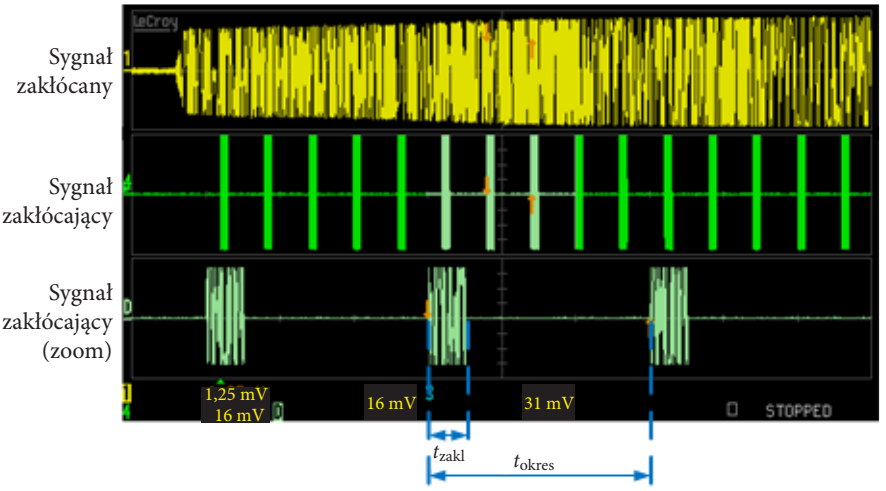
Rys. 6. Widmo amplitudowe sygnału zakłócanego i zakłócającego



t_{opoz} – czas od wykrycia sygnału celu do rozpoczęcia jego zakłócania
t_{zakl} – czas generacji pojedynczego impulsu zakłóceń

Rys. 7. Optymalizacja parametrów czasowych sygnału zakłócającego w trybie zakłócania synchronicznego transmisji pakietowych (cyfrowych)

zakłócania synchronicznego w przypadku transmisji ciągłych (analogowych) zaprezentowane zostało na rysunku 8. Jako przykład wykorzystano sygnał z radiotelefonów PMR. W tym przypadku również zastosowano parametr t_{zakl} w celu określenia minimalnego czasu trwania impulsu zakłócającego. Z uwagi na charakter sygnału zakłócanego, kolejne wyzwolenia następowały bezpośrednio po zakończeniu poprzedniego impulsu zakłócającego i w związku z tym t_{opoz} można interpretować jako t_{bez_zakl}. Uwzględniając ten fakt, optymalizacja polegała na doborze współczynnika wypełnienia sygnału zakłócającego określonego wzorem (4).



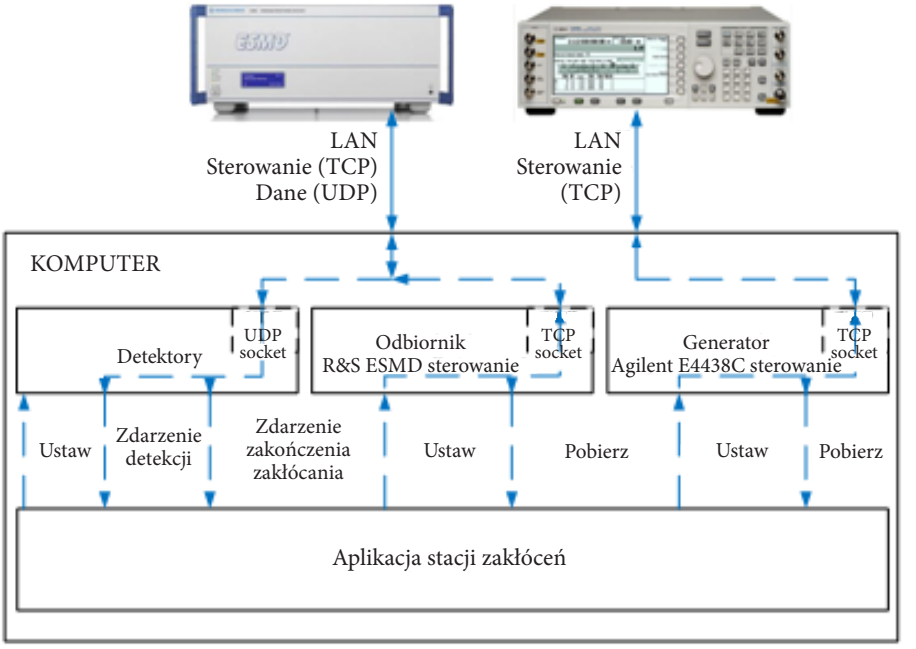
t_{zakl} – czas generacji pojedynczego impulsu zakłóceń
t_{okres} – okres powtarzania impulsów zakłócających

Rys. 8. Optymalizacja parametrów czasowych sygnału zakłócającego w trybie zakłócania synchronicznego transmisji ciągłych (analogowych)

5. Demonstrator stacji zakłóceń — zakłócanie asynchroniczne

Na bazie stanowiska laboratoryjnego opisanego w poprzednim punkcie powstał demonstrator stacji zakłóceń, składający się z generatora Agilent E4438C, odbiornika szerokopasmowego R&S ESMD oraz komputera z oprogramowaniem sterującym (rys. 9). W celu zdalnego sterowania urządzeniami wykorzystano interfejsy LAN oraz polecenia SCPI (ang. *Standard Commands for Programmable Instruments*) [4, 5], które umożliwiają ustawienie określonych parametrów oraz pobranie nastaw. W przypadku generatora mogą to być np.: poziom mocy wyjściowej, częstotliwość pracy, struktura sygnału zakłócającego. Dodatkową funkcjonalnością jest przesyłanie danych z monitorowania widma za pośrednictwem protokołu UDP (ang. *User Datagram Protocol*) z odbiornika R&S ESMD, które następnie przekazywane są do

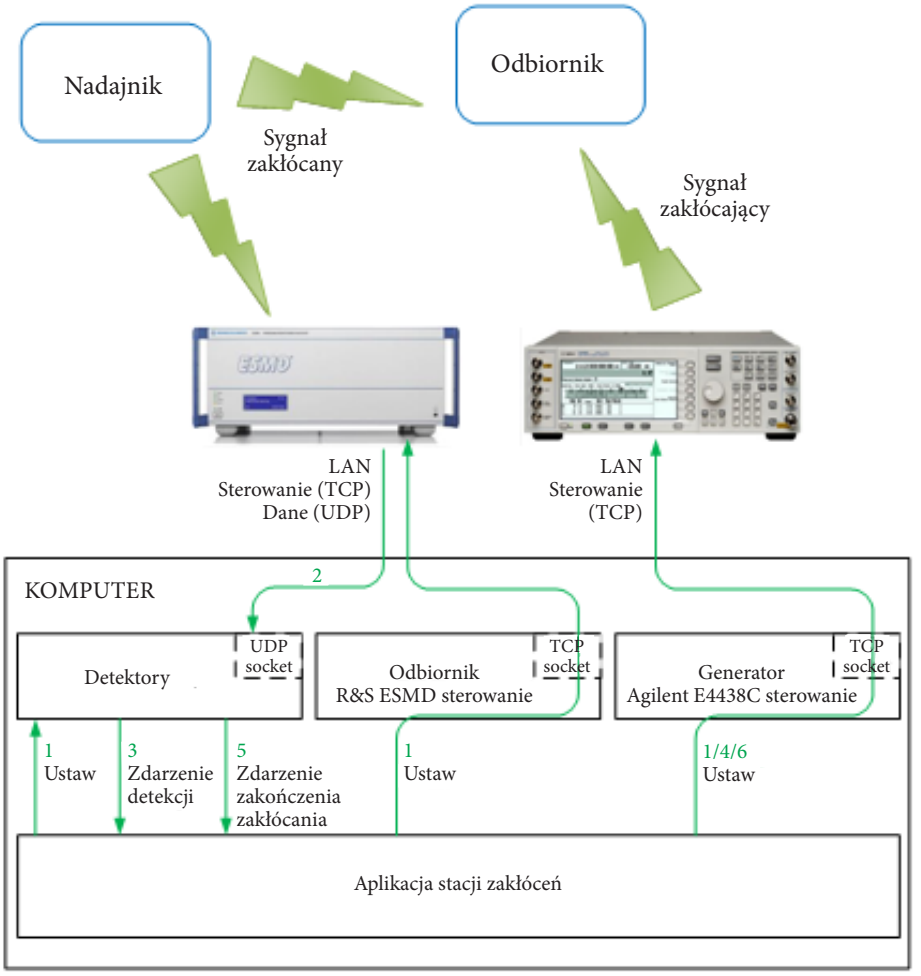
oprogramowania detektorów [6]. Taka konfiguracja stacji zakłóceń umożliwia realizację zakłócania zaporowego i odzewowego przy użyciu różnych struktur sygnału zakłócającego. Próbki IQ sygnału tworzone są w programie MATLAB, a następnie eksportowane do pamięci generatora. Demonstrator pracuje w trybie zakłócania asynchronicznego, w którym nie wymaga się synchronizacji z sygnałem zakłócanym.



Rys. 9. Schemat demonstratora stacji zakłóceń

Jako przykład działania demonstratora, na rysunku 10 przedstawiono kolejne etapy realizacji zadania odzewowego, np. zakłócania systemu GSM w oparciu o OpenBTS [7]. Podczas uruchomienia stacji urządzenia konfigurowane są według zapisanych ustawień inicjalizacyjnych. Następnie w pierwszym kroku realizacji zadania następuje ustawienie odpowiednich parametrów odbiornika i generatora oraz oprogramowania detektorów. Obejmują one nastawy m.in. struktury sygnału zakłócającego, skanowanych pasm częstotliwości, listy pasm częstotliwości obcych, czułości detektorów itp. Po właściwym zaprogramowaniu, odbiornik rozpoczyna wysyłanie danych z monitorowania widma do oprogramowania detektorów. Detektory, w momencie wykrycia sygnału znajdującego się w zdefiniowanym paśmie, wysyłają zdarzenie detekcji do aplikacji głównej, która z kolei steruje częstotliwością generatora Agilent, rozpoczynając zakłócanie celu. Mając na uwadze zadanie optymalizacji zdefiniowane w punkcie 3, polegające na minimalizacji czasu t_{calk}, zaimplementowano także funkcjonalność kontynuowania monitorowania, dzięki

której możliwe jest wykrycie zaniku sygnału zakłócanego. W takiej sytuacji oprogramowanie detektorów wysyła zdarzenie, które powoduje zakończenie zakłócania.



Rys. 10. Realizacja zadania odzewowego przez stację zakłóceń

6. Podsumowanie

Artykuł porusza aktualną w obszarze walki elektronicznej tematykę zakłócania transmisji przeciwnika. Niezwykle ważnym zagadnieniem jest poszukiwanie coraz bardziej skutecznych metod blokowania łączności wroga, które jest również formą ochrony przed improwizowanymi ładunkami wybuchowymi detonowanymi drogą radiową.

Jako cel optymalizacji sygnału zakłócającego przyjęto minimalizację jego energii, która determinuje minimalizację całkowitego czasu generacji zakłóceń. Zestawione stanowisko laboratoryjne pozwoliło na dobór tych parametrów dla badanych systemów. Bardzo ważnym atutem przedstawionego stanowiska jest praca w trybie zakłócania synchronicznego, dzięki czemu możliwa jest analiza poszczególnych systemów pod kątem zakłócania inteligentnego, w którym zakłóceniom poddawane są tylko wybrane fragmenty sygnału. Zaprezentowany demonstrator programowalnej stacji zakłóceń umożliwia pracę w jednym z trzech trybów: zakłócania zaporowego, zakłócania odzewowego lub monitorowania widma. Realizuje on zakłócanie asynchroniczne z wykorzystaniem wybranego waveformu na jednej częstotliwości. Istotną zaletą tego demonstratora jest wykorzystanie urządzeń, których parametry mogą być definiowane za pomocą sterowania programowego, realizowanego przez aplikację główną zainstalowaną na komputerze. Warto także zwrócić uwagę na korzyść wynikającą z możliwości tworzenia własnych struktur sygnałów zakłócających.

W docelowej wersji stacji zakłóceń należy rozważyć wykorzystanie dedykowanych urządzeń pozwalających na minimalizację czasu reakcji systemu oraz wprowadzić kilka torów odbiorczo-nadawczych. Ze względu na fakt, że przebadane systemy stanowią zaledwie niewielką część dostępnych rozwiązań konieczne jest przeprowadzenie kolejnych testów w celu znalezienia skutecznej metody zakłócania jak najszerszej gamy systemów.

Zaprezentowany demonstrator został wykorzystany w systemie kontroli łączności radiowej przeciwnika realizowanego w ramach projektu ICAR (ang. *Intelligent Control of Adversary Radio-communications*) [8].

Praca zrealizowana w ramach projektu A-0935-RT-GC *Intelligent Control of Adversary Radio-communications (ICAR)*, European Defence Agency.

LITERATURA

[1] A. Graham, *Communications, Radar And Electronic Warfare*, Willey, 2011, 95-100.

[2] D.L. Adamy, *Tactical Battlefield Communications Electronic Warfare*, Artech House, 2009, 251-273.

[3] R. Poisel, *Modern Communications Jamming Principles and Techniques*, Second Edition, Artech House, 2011, 467-503.

[4] *E4438C ESG Vector Signal Generator*, SCPI Command Reference, vol. 1.

[5] Rohde&Schwarz ESMD Wideband Monitoring Receiver, Manual.

[6] M. Kryk, J. Łopatka, *Efektywna metoda monitoringu widma do wykrywania sygnałów wyzwalających IED*, KNTWE, 2012.

[7] A. Kaszuba, R. Chęciński, J. Łopatka, W*ykorzystanie platformy radia programowalnego USRP do przechwytywania informacji o użytkownikach GSM*, KNTWE, 2012.

[8] J. Łopatka, R. Chęciński, A. Kaszuba, R. Krawczak, *Inteligentna kontrola łączności przeciwnika z wykorzystaniem bezzałogowej platformy lądowej DROMADER*, KNTWE, 2012.

K. MALON, J. ŁOPATKA

Demonstrator of software controlled jamming station

Abstract. In the field of electronic warfare, a very important issue is to search more and more efficient methods for controlling enemy radio communications. The main issue related to this topic is efficient jamming of communication systems and protection against radio controlled Improvised Explosive Devices (IEDs). The jamming stations used for these purposes can be mounted either on typical military vehicles or on board of Unmanned Ground Vehicles (UGVs).

The article describes the basic jamming techniques including features and characteristics which indicate the scope of their use. Then, the test bed to define optimal parameters of jamming signal is presented. The goal of optimization was to minimize jamming signal energy, keeping their efficiency. Their parameters include in particular: the jamming signals time characteristics (e.g. maximum jamming delay time, minimum jamming signal duration, repetition period) and their spectral properties (e.g. noise signal, sweep). Presented test bed was also used to test synchronous jamming, triggered by successive packets of transmitted data. The next part of the paper contains characteristic of jamming station demonstrator, consisting of the following elements:

— arbitrary Agilent E4438C signal generator,
— Rohde & Schwarz ESMD wideband receiver,
— computer with control software.

In this case, an asynchronous jamming, without synchronization to data, was applied. As an example of jamming, realization of response jamming is presented.

Keywords: telecommunication, electronic warfare, jamming, improvised explosive devices