



**Politechnika
Śląska**

ROZPRAWA DOKTORSKA

System radioelektronicznej detekcji i przeciwdziałania bezzałogowym
statkom powietrznym

mgr inż. Przemysław FLAK

PROMOTOR

dr hab. inż. Roman Czyba, prof. PŚ

Wydział Automatyki, Elektroniki i Informatyki

Gliwice 2025

Streszczenie

Historia rozwoju bezzałogowych statków powietrznych, zwanych także dronami, pokazuje, że mimo początkowego przeznaczenia ściśle związanego z wojskowością, zaistniały postęp technologiczny przyczynił się do znacznego wzrostu ich cywilnych zastosowań. Wprowadzenie dronów do użytku komercyjnego otworzyło zupełnie nowe możliwości dla wielu gałęzi gospodarki, dzięki wyjątkowej wszechstronności tych urządzeń. Rosnące zapotrzebowanie na usługi powietrzne, wysoka dostępność amatorskich rozwiązań i niski próg wejścia w świat bezzałogowców wpłynęły niestety również na powstanie nowej kategorii zagrożeń, nie tylko dla obiektów infrastruktury krytycznej, ale także dla sfery życia codziennego.

Celem niniejszej rozprawy jest przegląd metod oraz zaproponowanie sposobu wykrywania oraz przeciwdziałania niepożądanym działaniom wynikającym z użycia komercyjnych bezzałogowych statków powietrznych. Podejście radioelektroniczne, opierające się na zdolności do identyfikacji i klasyfikacji źródeł promieniowania elektromagnetycznego, a w konsekwencji zakłócania ich działania, zostało wybrane jako przedmiot szerszej analizy. Mimo iż zasięg działania systemów antydronowych z tej kategorii definiuje się często na kilka kilometrów, to przeszkody terenowe, warunki propagacyjne oraz zabudowa gospodarcza wpływają jednak znacząco na jego ograniczenie. Dodatkowo koszt tych rozwiązań, połączony z zapotrzebowaniem na duże moce obliczeniowe, powoduje trudności ze skalowaniem tego podejścia w aplikacjach, gdzie wymagana jest ochrona dużego obszaru.

Prezentowana praca badawcza obejmuje nie tylko ewaluację znanych technik i algorytmów, ale także opracowanie autorskiego rozwiązania, które będzie dostosowane do konkretnego scenariusza operacyjnego. Ważnym aspektem pracy jest również wytworzenie fizycznego prototypu urządzenia opartego na łatwo dostępnych komponentach oraz określenie jego możliwości w odniesieniu do danych warunków operacyjnych. Koncepcja rozproszonej sieci detektorów i efektorów z lokalnym przetwarzaniem, ograniczającym zapotrzebowanie na bardzo wysoką przepustowość łącza danych, przebadana została w warunkach symulacyjnych oraz zbliżonych do rzeczywistych.

Bazując na komercyjnym układzie elektronicznym, w ramach prac dokonano zmian w oprogramowaniu, które pozwalały na zwiększenie udziału warstwy sprzętowej w procesach detekcji sygnałów radiowych opartych na zapisie czasowo-częstotliwościowym. Zaproponowano także algorytmy identyfikacji transmisji pochodzących od statków bezzałogowych z wykorzystaniem technik uczenia maszynowego, co przeanalizowane zostało zarówno na otwartej, jak i własnej bazie sygnatur. W ostatniej części pracy zamieszczono eksperymenty potwierdzające zdolności efektorów do zakłócania sygnałów nawigacji satelitarnej oraz tych używanych do zdalnego sterowania systemami bezzałogowymi. W wyniku prac powstał prototyp, który może służyć zarówno jako samodzielny wskaźnik obecności niepożądanych obiektów w okolicy, jak i element niezbędny do realizacji koncepcji architektury rozproszonej.

Abstract

The history of the development of unmanned aerial vehicles, also known as drones, shows that, despite their initial military-oriented design, technological advances have contributed to a significant increase in their civilian deployment. The introduction of drones for commercial applications has opened up entirely new opportunities for many sectors of the industry, due to the exceptional versatility of these devices. Unfortunately, the growing demand for aerial services, the high availability of amateur solutions, and the low barrier of entry into the world of unmanned aerial vehicles have also unleashed a new category of threats, not only to critical infrastructure but also to everyday life.

The aim of this dissertation is to review methods and provide a solution for detecting and counteracting malicious activities resulting from the use of commercial unmanned aerial vehicles. The radio-electronic approach, based on the ability to identify and classify sources of electromagnetic emissions and, consequently, to disrupt their operation, has been selected for further analysis. Although the range of counter-drone systems in this category is often defined as several kilometres, field conditions, propagation effects, and urban development significantly limit its effectiveness. In addition, the cost of these solutions, combined with the need for high computing power, makes it difficult to scale this approach in applications where large areas need to be protected.

The featured research work covers not only the evaluation of known techniques and algorithms but also the development of a proprietary solution tailored to a specific operational scenario. An important aspect of the project is also the creation of a physical prototype of a device based on off-the-shelf components and the characterisation of its capabilities in relation to specific operational conditions. The concept of a distributed network of detectors and effectors with local processing, limiting the need for very high data link throughput, has been tested in simulated and near-real conditions.

Based on a commercial electronic circuit, the author made changes to the software to increase the contribution of the hardware layer in the processes of detecting radio signals based on time-frequency recordings. Algorithms for identifying transmissions from unmanned aerial vehicles using machine learning techniques were also proposed, which were analysed with reference to either an open or proprietary signature database. The last part of the work presents experiments confirming the effector's ability to jam satellite navigation signals and those used for remote control of drone systems. The result of this thesis is a prototype that can serve both as a standalone indicator of the presence of unwanted objects in the vicinity and as an essential element for the implementation of the distributed architecture concept.

Spis treści

Lista skrótów	1
1 Wstęp	5
1.1 Uzasadnienie podjęcia tematu	6
1.2 Problematyka rozprawy	7
1.3 Cel, tezy i zakres rozprawy	8
1.4 Dorobek naukowy autora	10
1.5 Przegląd zawartości rozprawy	11
2 Detekcja i przeciwdziałanie bezzałogowym statkom powietrznym	13
2.1 Metody detekcji	13
2.1.1 Akustyczne	13
2.1.2 Wizyjne	14
2.1.3 Radarowe	15
2.1.4 Lidarowe	16
2.1.5 Radiowe	16
2.1.6 Heterogeniczne	17
2.2 Metody przeciwdziałania	17
2.2.1 Prawne i administracyjne	18
2.2.2 Kinetyczne	18
2.2.3 Radiowe	19
2.2.4 Energetyczne	20
3 Wprowadzenie do tematyki walki elektronicznej	21
3.1 Wstęp	21
3.2 Analiza i przetwarzanie sygnałów	22
3.2.1 Ciągła transformacja Fouriera	23
3.2.2 Dyskretna transformacja Fouriera	23
3.2.3 Krótkoczasowa transformacja Fouriera	24
3.3 Tor komunikacyjny	25
3.3.1 Radiowy kanał propagacyjny	25

3.3.2	Modelowanie kanału	27
3.4	Detekcja sygnałów radiowych	28
3.4.1	Detekcja energii	29
3.4.2	Detekcja oparta na cechach charakterystycznych	31
3.4.3	Detekcja oparta na entropii	32
3.5	Sztuczna inteligencja w systemach rozpoznania radiowego	33
3.5.1	Klasyczne i głębokie uczenie maszynowe	34
3.5.2	Topologie wybranych sieci neuronowych	35
3.5.3	Ocena i porównywanie modeli	36
3.6	Zakłócanie sygnałów radiowych	38
3.6.1	Podstawowe techniki zakłócania	40
3.6.2	Wybrane strategie zakłócania	41
4	Analiza bazy wiedzy w kontekście wybranej metody detekcji i przeciwdziałania bezzałogowym statkom powietrznym	43
4.1	Charakterystyka komercyjnych dronów	43
4.1.1	Przegląd rynku	44
4.1.2	Kanał sterowania i transmisji obrazu	45
4.1.3	Odbiornik nawigacji satelitarnej	48
4.1.4	Nadajnik zdalnej identyfikacji	50
4.2	Przegląd prac z zakresu wykrywania BSP	52
4.2.1	Protokół radiowy	52
4.2.2	Dziedzina czasu	53
4.2.3	Dziedzina częstotliwości	54
4.2.4	Spektrogram	55
4.3	Przegląd prac z zakresu przeciwdziałania BSP	57
4.3.1	Zakłócanie sygnałów nawigacji satelitarnej	57
4.3.2	Zakłócanie sygnałów sterowania	60
5	Prototyp sensora i efektora radioelektronicznego	65
5.1	Koncepcja radia programowalnego	65
5.1.1	Budowa wewnętrzna	65
5.1.2	Porównanie dostępnych urządzeń	68
5.1.3	Oprogramowanie obsługowe	71
5.2	Modyfikacje funkcjonalne klasycznego SDR	72
5.2.1	Wykorzystanie pełnej częstotliwości próbkowania	73
5.2.2	Wsparcie sprzętowe obliczeń FFT	73
5.2.3	Metody aproksymacyjne dostosowane do FPGA	75
5.2.4	Modyfikacje toru nadawczego	78
5.2.5	Pomiary laboratoryjne	78

5.2.6	Eksperymenty na sygnałach rzeczywistych	81
5.3	Przestrzajanie szerokopasmowe	82
5.3.1	Analiza dostępnych rozwiązań	84
5.3.2	Implementacja metody w torze odbiorczym	85
5.3.3	Implementacja metody w torze nadawczym	89
5.3.4	Rozszerzenie zakresu częstotliwości	90
5.3.5	Pomiary laboratoryjne	91
5.3.6	Eksperymenty na sygnałach rzeczywistych	93
6	Badania w dziedzinie detekcji	97
6.1	Wprowadzenie	97
6.1.1	Modelowanie scenariusza wtargnięcia	97
6.1.2	Strategia pracy rozproszonej	100
6.1.3	Przegląd istniejących baz sygnatur dronowych	102
6.2	Techniki analizy widma	104
6.2.1	Detekcja klasyczna	105
6.2.2	Klasyfikacja binarna	112
6.2.3	Detekcja i klasyfikacja jednorodna	117
6.2.4	Badania w środowisku rzeczywistym	122
7	Badania w dziedzinie przeciwdziałania	125
7.1	Sygnały nawigacji satelitarnej	125
7.1.1	Modelowanie scenariusza zakłócania	126
7.1.2	Charakterystyka podatności odbiornika GNSS	129
7.1.3	Eksperymenty	132
7.2	Sygnały kierowania i kontroli	137
7.2.1	Modelowanie scenariusza zakłócania	138
7.2.2	Charakterystyka podatności odbiornika OFDM	140
7.2.3	Eksperymenty	142
8	Podsumowanie	147
8.1	Wnioski z realizowanych prac	147
8.2	Ocena stopnia realizacji przyjętych celów	153
8.3	Kierunki dalszych badań	155
	Spis rysunków	160
	Spis tabel	161
	Bibliografia	181

Lista skrótów

ABS	absolute value
ACCST	Advanced Continuous Channel Shifting Technology
ACK	acknowledgement
ADC	Analog Digital Converter
AFE	Analog Front-End
AFHDS	Automatic Frequency Hopping Digital System
AGC	Automatic Gain Control
AI	Artificial Intelligence
ANN	Artificial Neural Networks
API	Application Programming Interface
AWGN	Additive White Gaussian Noise
BER	Bit Error Rate
BPSK	Binary Phase Shift Keying
BRAM	Block Random Access Memory
BSP	Bezzałogowy Statek Powietrzny
CAF	Cross Ambiguity Function
CFAR	Constant False Alarm Rate
CLB	Configurable Logic Block
CNN	Convolutional Neural Network
COCO	Common Objects in Context
CORDIC	Coordinate Rotation Digital Computer
CPU	Central Processing Unit
CW	Constant Wave
DAC	Digital Analog Converter
dBFS	Decibels Relative to Full Scale
DDFS	Direct Digital Frequency Synthesis
DFT	Discrete Fourier Transform
DL	Deep Learning
DMA	Direct Memory Access
DNN	Deep Neural Network

DoS Denial of Service
DSP Digital Signal Processing
DSSS Direct Sequence Spread Spectrum
DT Decision Trees
EVM Error Vector Magnitude
FASST Futaba Advanced Spread Spectrum Technology
FCME Forward Consecutive Mean Excision
FFT Fast Fourier Transform
FHSS Frequency-Hopping Spread Spectrum
FIFO First In First Out
FPGA Field Programmable Gate Array
FSK Frequency-Shift Keying
FSL Free Space Loss
GFLOP Giga Floating Point Operations Per Second
GFSK Gaussian Frequency Shift Keying
GNSS Global Navigation Satellite System
GPIF General Programmable Interface
IC Integrated Circuit
IoU Intersection-over-Union
IQ In-phase, Quadrature
ISM Industrial, Scientific, and Medical
JSR Jamming to Signal Ratio
KNN K-Nearest Neighbours
LAN Local Area Network
LNA Low Noise Amplifier
LOD Leading-One Detector
LOS Line-of-Sight
LSTM Long Short-Term Memory
LTE Long Term Evolution
MAC Media Access Control
MAE Mean Absolute Error
mAP Mean Average Precision
MFLOP Milion Floating Point Operations Per Second
ML Machine Learning
MSE Mean Square Error
MUX multiplexer
NB Naive Bayes
NCO Numerically Controlled Oscillator
NLOS Non Line-of-Sight

NMSE Normalized Mean Square Error
NPAQM Non-parametric Amplitude Quantization Method
OFDM Orthogonal Frequency-Division Multiplexing
PC Personal Computer
PLL Phase Locked Loop
PRN Pseudorandom Noise
PSK Phase Shift Keying
QAM Quadrature Amplitude Modulation
R-CNN Region-based Convolutional Neural Network
RAM Random Access Memory
RC Remote Contoled
RCS Radar Cross-Section
RDF Random Decision Forests
REG register
RNN Recurrent Neural Networks
ROHT Recursive One-sided Hypothesis Testing
RSSI Received Signal Strength Indication
SBC Single Board Computer
SDR Software Defined Radio
SJR Signal to Jamming Ratio
SNR Signal to Noise Ratio
SPI Serial Peripheral Interface
STFT Short-Time Fourier Transform
SVD Singular Value Decomposition
SVM Support Vector Machines
UART Universal Asynchronous Receiver-Transmitter
USB Universal Serial Bus
VGG Visual Geometry Group
VHDL Very High Speed Integrated Circuit Hardware Description Language
Wi-Fi Wireless Fidelity
WRE Walka Radioelektroniczna
YOLO You Only Look Once
ZIF Zero Intermediate Frequency

Rozdział 1

Wstęp

Bezzałogowy Statek Powietrzny (BSP) jest maszyną, która do wykonywania zadań lotniczych nie wymaga na pokładzie obecności załogi, może być pilotowana zdalnie przez operatora lub działać w sposób autonomiczny. Historia rozwoju tych urządzeń jest wielowątkowa, aczkolwiek niewątpliwie od pierwszego udanego lotu braci Wright w 1903 roku człowiek chciał wykorzystać maszyny lotnicze do zastosowań militarnych. Zestawiając to z pierwszym sterowanym drogą radiową urządzeniem, które zaprezentował Nikola Tesla w 1898 roku, możemy mówić o rozpoczęciu ery systemów bezzałogowych, przypadającej na początek XX wieku [1].

W Wielkiej Brytanii eksperymenty z prototypowym wykorzystaniem płatowca Ruston Proctor Aerial Target już w 1917 roku miały na celu bojowe użycie przeciwko sterowcom, a torpeda lotnicza ze Stanów Zjednoczonych, znana jako Kettering Bug, po raz pierwszy została oblatana rok później. Pierwotnym zastosowaniem małych samolotów sterowanych drogą radiową było jednak pozorowanie celów na potrzeby ćwiczeń zespołów obrony przeciwlotniczej. Pierwsza seryjnie produkowana flota bezzałogowców weszła do służby w 1935 roku. Był to przełomowy model DH.82 Queen Bee, który zapoczątkował zwyczaj nazywania maszyn bezzałogowych dronami - od angielskiego słowa „drone” oznaczającego trutnia. W latach pięćdziesiątych skonstruowano pierwszy BSP przeznaczony ściśle do zadań rozpoznawczych o nazwie MQM-57 Falconer. Model ten, wyprodukowany w liczbie ponad 1500 sztuk, stał się podstawowym dronem rozpoznawczym dla armii amerykańskiej aż do lat siedemdziesiątych. W tamtym momencie coraz więcej państw zaczęło dostrzegać drzemiący w systemach bezzałogowych potencjał i rozpoczynać własne programy rozwoju takiej floty. Aktualnie liczbę maszyn tego typu pozostających w aktywnej służbie na świecie można wyrazić w dziesiątkach tysięcy.

Pojawienie się nowych technologii ofensywnych zawsze niesie za sobą także konieczność rozwoju środków przeciwdziałania. Początkowo platformy bezzałogowe nie odbiegały rozmiarami od platform załogowych, a nawet były ich zmodyfikowanymi wersjami z dodatkowymi systemami zdalnej kontroli. W rezultacie ówczesne systemy przeciwlotnicze charakteryzowały się podobną skutecznością w obu przypadkach. Do tej pory zaawanso-

wane techniki stosowane do ochrony przestrzeni powietrznej opracowywano w większości z myślą o platformach załogowych oraz optymalizowano pod kątem wykrywania, śledzenia i likwidacji dużych, szybko poruszających się obiektów. Wzrost skali integracji układów półprzewodnikowych oraz rozwój nowych technologii materiałowych wpłynął jednak znacząco na miniaturyzację dronów w ostatnich latach. Dodatkowo zdolność do operowania na małych wysokościach i przy niskich prędkościach stworzyła poważną lukę w systemach ochrony.

W badaniu rynku przeprowadzonym w 2015 roku naukowcy z Sandia National Laboratories zidentyfikowali jedynie kilkanaście gotowych do wdrożenia systemów dedykowanych przeciwdziałaniu dronom [2]. Po dekadzie różnorodność produktów w tej kategorii można szacować już w setkach. W tym czasie nie tylko sama technologia aparatów bezzałogowych znacznie się rozwinęła, ale również baza wiedzy na temat ich operacyjnego użycia stała się większa. Rosnąca liczba publikacji naukowych i programów rozwojowych wspierających ewolucję systemów antydronowych wskazuje, że kilka ważnych problemów wciąż nie zostało rozwiązanych i istnieje miejsce na dalsze badania.

1.1 Uzasadnienie podjęcia tematu

Historia bezzałogowych statków powietrznych pokazuje, że początkowym akcelerato-rem rozwoju tej technologii zdecydowanie był sektor wojskowy. Rosnąca popularność smartfonów, powszechna dostępność sygnałów nawigacji satelitarnej, postępy technologiczne w komunikacji bezprzewodowej i obrazowaniu przyczyniły się do znacznego wzrostu wartości rynku dronów cywilnych. Od momentu, gdy Federalna Administracja Lotnictwa Stanów Zjednoczonych przyznała pierwszą komercyjną licencję w 2006 roku, globalna świadomość tej technologii zwiększa się w ogromnym tempie. Według najnowszego raportu FAA (ang. *Federal Aviation Administration*) liczba dronów rekreacyjnych w Stanach Zjednoczonych ma osiągnąć szczyt na poziomie około 1,92 miliona jednostek do 2028 roku, przy 472 tysiącach zarejestrowanych operatorów [3]. Dla odniesienia, w Polsce, zgodnie z danymi Urzędu Lotnictwa Cywilnego, na koniec 2024 roku zarejestrowanych było ponad 300 tysięcy operatorów, co obrazuje również skalę tej aktywności w naszym kraju [4].

Wprowadzenie systemów bezzałogowych do użytku cywilnego otworzyło zupełnie nowe obszary zastosowań w wielu gałęziach gospodarki dzięki wyjątkowym możliwościom i wszechstronności tych urządzeń. Dziś modelowym reprezentantem kategorii komercyjnych bezzałogowych statków powietrznych możemy uznać obiekt o masie od kilkuset gramów do kilku kilogramów i wielowirnikowym układzie napędowym. Konstrukcje te są łatwe w sterowaniu, oferują możliwość stabilnego zawisu w powietrzu i nawet do kilku kilometrów łączności bezprzewodowej. Nie sposób wymienić wszystkich dziedzin, na które w ostatnich latach miała wpływ dronowa rewolucja. Do najważniejszych należą między innymi rolnictwo, logistyka oraz szeroko pojęty temat inspekcji i nadzoru. Poza zastosowaniami

komercyjnymi znajdują się również te związane z ratowaniem życia, takie jak transport krwi i materiałów medycznych, czy poszukiwanie zaginionych w kłęskach żywiołowych.

Rosnące zapotrzebowanie na usługi powietrzne, wysoka dostępność amatorskich rozwiązań i niski próg wejścia w świat bezzałogowców wpłynęły niestety również na powstanie nowej kategorii zagrożeń bezpieczeństwa. Wprowadzenie odpowiednich przepisów oraz edukacja użytkowników mogą ograniczyć większość nieintencjonalnych zdarzeń związanych z dronami. Niemniej jednak nadal istnieje strefa, w której drony mogą być wykorzystywane w celu przeprowadzenia bezprawnej ingerencji czy spowodowania szkód w obiektach infrastruktury krytycznej.

Pierwsze wzmianki o poważnych incydentach z użyciem dronów komercyjnych sięgają 2014 roku, co zgrywa się z datą premiery jednego z najbardziej rozpoznawalnych modeli w tej kategorii. Dotyczą one głównie obecności urządzeń w okolicach lotnisk, a nawet wskazują na poważną możliwość kolizji z samolotem pasażerskim [5]. Do najpopularniejszych zdarzeń tego rodzaju można zaliczyć to z 2018 roku, kiedy to na lotnisku Gatwick w pobliżu Londynu setki lotów zostały odwołane po doniesieniach o obserwacjach dronów w pobliżu pasa startowego. To było największe zakłócenie, jakie miało miejsce na tym lotnisku od czasu wybuchu wulkanu na Islandii w 2010 roku [6]. Nielegalne wykorzystanie systemów bezzałogowych obejmuje również wtargnięcia na teren elektrowni jądrowych [7], przemysł [8] oraz akty terroryzmu [9].

Oprócz przytoczonych powyżej poważnych incydentów coraz częstsze stają się również zagrożenia związane z naruszeniem prywatności i dóbr osobistych. Ponieważ większość powszechnie dostępnych dronów konsumenckich zawiera wysokiej jakości kamery z możliwością bezpośredniej transmisji obrazu, mogą być one wykorzystywane do nękania lub prześladowania ludzi [10]. Powyższe przykłady podkreślają znaczenie opracowywania automatycznych systemów monitorowania przestrzeni powietrznej, które mogą działać zarówno w scenariuszach wysoko wyspecjalizowanych, jak i w bardziej ogólnych warunkach.

1.2 Problematyka rozprawy

Mimo wzrostu konkurencji na rynku wykrywania i przeciwdziałania bezzałogowym statkom powietrznym, dostępność tych systemów dla osób prywatnych jest utrudniona z uwagi na wysoki koszt rozwiązania. Póki w aspekcie neutralizacji ograniczenia mogą wynikać z uwarunkowań prawnych czy etycznych, to już sama detekcja obecności intruza może ułatwić rozwiązanie wielu podstawowych problemów. Powtarzające się w bliskim otoczeniu autora zdarzenia związane ze stalkingiem przy użyciu dronów były jedną z inspiracji do podjęcia tego zagadnienia. Dodatkowo, wybór obszaru badawczego, który dotyczy techniki związanej z łącznością radiową, wyklarował się, gdy podczas prześladowania bezpośrednia kontrola drona oraz transmisja obrazu na żywo okazały się nieodłącznymi elementami nielegalnych działań.

System zaopatrzenia w energię elektryczną można niewątpliwie uznać za część infrastruktury krytycznej dla bezpieczeństwa państwa. Skuteczną formą ataku w tym przypadku może być wytworzenie zwarcia przy użyciu platformy latającej z podwieszonym przewodem miedzianym [11]. Ze względu na dużą liczbę punktów węzłowych i rozległość sieci przesyłowych, pokrycie tego obszaru ochroną stanowi wyzwanie. Dodatkowo należy zaznaczyć, iż każdy wielkopowierzchniowy obiekt przemysłowy czy port lotniczy charakteryzuje się specyficznymi uwarunkowaniami, które uniemożliwiają opracowanie zunifikowanego rozwiązania [12].

Większość obecnie dostępnych systemów antydronowych ma zasięg o promieniu kilku kilometrów oraz składa się z zestawu detektorów centralnych i stacji analiz. Zdarzają się systemy, w których stosuje się kilka elementów detekcyjnych w celu przeprowadzenia triangulacji dla pozycjonowania intruza. Skuteczność większości detektorów zależy od bezpośredniej widoczności poszukiwanego obiektu. Uwarunkowania terenowe, warunki propagacyjne oraz zabudowa gospodarcza wpływają jednak znacząco na ograniczenie ich zasięgu [13].

Istotnym problemem we wszystkich analizowanych układach wykrywania bezzałogowych statków powietrznych jest złożoność operacji obliczeniowych i konieczność pracy w czasie rzeczywistym. W budowaniu rozległej sieci detekcyjnej nie bez znaczenia jest również ogromna ilość danych niezbędnych do przesłania z sensorów do stacji analiz, często wykraczająca poza możliwości istniejącej infrastruktury. Multiplikowanie wydajnych jednostek obliczeniowych stoi natomiast w opozycji do ekonomicznego aspektu podejścia do tematu.

Mając na uwadze powyższe aspekty, można zaproponować ideę rozproszonej sieci detektorów i efektorów z lokalnym przetwarzaniem, ograniczającym zapotrzebowanie na bardzo wysoką przepustowość łącza danych. Infrastruktura mogłaby potencjalnie składać się z dużej liczby węzłów czujnikowych wraz z centrum fuzji danych, zdolnym do przetwarzania zarówno fragmentarycznych, jak i niejednoznacznych danych wejściowych [14]. Do zbadania pozostaje poziom kompromisu pomiędzy wymaganą dla danej aplikacji skutecznością a możliwościami obecnie dostępnych, niedrogich elementów elektronicznych.

1.3 Cel, tezy i zakres rozprawy

Celem niniejszej rozprawy jest analiza metod rozpoznawania i przeciwdziałania niepożądanym komercyjnym bezzałogowym statkom powietrznym. Podejście radioelektroniczne, opierające się na zdolności do identyfikacji i klasyfikacji źródeł promieniowania elektromagnetycznego, a w konsekwencji zakłócania ich działania, zostało wybrane jako przedmiot szerzej zakrojonych badań. Praca badawcza obejmie nie tylko ewaluację znanych algorytmów, ale przede wszystkim opracowanie autorskiego rozwiązania, które będzie dostosowane do konkretnego scenariusza operacyjnego. Ważnym aspektem pracy jest również wytworze-

nie prototypu urządzenia oraz określenie jego możliwości w odniesieniu do rzeczywistych warunków operacyjnych. Powyższe cele prowadzą do sformułowania następujących tez dysertacji:

Możliwa jest realizacja układu detekcji oraz zakłócania operacji bezzałogowych statków powietrznych na podstawie informacji z modułu radia definiowanego programowo.

Możliwa jest realizacja systemu detekcji oraz zakłócania komercyjnych dronów, bazującego na gotowych układach elektronicznych i modyfikacji oryginalnego oprogramowania.

Zastosowanie architektury sprzętowo-programowej i zwiększenie udziału macierzy programowalnych bramek logicznych w przetwarzaniu sygnałów, w porównaniu do klasycznej koncepcji radia programowalnego, pozwoli na optymalizację procesu detekcji oraz zakłócania.

Optymalizacja procesu detekcji, pod względem minimalizacji czasu przetwarzania, może zostać zrealizowana dzięki analizie tylko fragmentów ramek radiowych.

System rozproszonej detekcji będzie miał przewagę w terenie zabudowanym nad systemem z detektorem centralnym oraz pozwoli na stworzenie skalowalnej sieci automatycznego nadzoru.

Zakres pracy obejmuje:

- przegląd sposobów wykrywania bezzałogowych statków powietrznych i ich zwalczania z uwzględnieniem różnych technik obserwacji przestrzeni
- analizę literatury pod kątem technik detekcji i zakłócania zorientowaną na podejście radioelektroniczne
- implementację funkcjonalności programowych rozszerzających możliwości komercyjnego urządzenia radia programowalnego
- przygotowanie oraz przebadanie prototypu elementu sensora i efektora zoptymalizowanego dla proponowanej koncepcji
- modelowanie propagacji fal radiowych w odniesieniu do przykładowego obiektu infrastruktury krytycznej
- przygotowanie bazy danych sygnatur radiowych na potrzeby trenowania i ewaluacji modeli uczenia maszynowego
- opracowanie i przebadanie metod detekcji dopasowanej do przyjętej koncepcji

- adaptację znanych metod zakłócania sygnałów radiowych do możliwości sprzętowych prototypu
- badania eksperymentalne opracowanych technik w warunkach laboratoryjnych oraz zbliżonych do rzeczywistych

1.4 Dorobek naukowy autora

W procesie realizacji badań na potrzeby dysertacji powstały trzy artykuły, opublikowane w recenzowanych czasopismach oraz jeden w monografii konferencyjnej. Materiały i eksperymenty w nich zawarte stanowią podstawę przedstawianego opracowania:

- Flak Przemysław, "Drone Detection Sensor With Continuous 2.4 GHz ISM Band Coverage Based on Cost-Effective SDR Platform". W: *IEEE ACCESS* 9 (2021), s. 114574-114586 [15]. 100 punktów MNiSW, 3,6 Impact Factor.
- Flak Przemysław, "Hardware-Accelerated Real-Time Spectrum Analyzer With a Broadband Fast Sweep Feature Based on the Cost-Effective SDR Platform". W: *IEEE ACCESS* 10 (2022), s. 110934-110946 [16]. 100 punktów MNiSW, 3,6 Impact Factor.
- Flak Przemysław i Czyba Roman, "System detekcji oraz przeciwdziałania bezzałogowym statkom powietrznym przy użyciu technik walki radioelektronicznej". W: *Automatyzacja procesów dyskretnych. Teoria i zastosowania. T. 1 / Świerniak Andrzej, Krystek Jolanta (red.), 2022, Gliwice, Wydawnictwo Politechniki Śląskiej, s.59-62, ISBN 978-83-7880-854-1 [17]. 20 punktów MNiSW.*
- Flak Przemysław i Czyba Roman, "RF Drone Detection System Based on a Distributed Sensor Grid With Remote Hardware-Accelerated Signal Processing". W: *IEEE ACCESS* 11 (2023), s. 138759-138772 [18]. 100 punktów MNiSW, 3,6 Impact Factor.

Aspekt naukowy uzupełniają także wygłoszone referaty:

- Akademia Wojsk Lądowych im. Tadeusza Kościuszki we Wrocławiu, referat pod tytułem „Wykorzystanie nowoczesnych technologii we flocie Bezzałogowych Systemów Powietrznych produkcji WB Group”, Wrocław, 25.03.2021.
- Politechnika Śląska, Priorytetowy Obszar Badawczy 5, podobzdar 6, referat pod tytułem „Nowoczesne technologie dla przeciwdziałania współczesnemu zagrożeniu ze strony bezzałogowych statków powietrznych”, Gliwice, 24.06.2021.
- Politechnika Śląska, Priorytetowy Obszar Badawczy 5, podobzdar 6, referat pod tytułem „A distributed electromagnetic pollution measurement system based on Software Defined Radio technology”, Gliwice, 30.06.2022.

- XXII Krajowa Konferencja Automatyzacji Procesów Dyskretnych, referat pod tytułem „System detekcji oraz przeciwdziałania bezzałogowym statkom powietrznym przy użyciu technik walki radioelektronicznej”, Zakopane, 21-24.09.2022.

1.5 Przegląd zawartości rozprawy

Rozprawa została podzielona na osiem rozdziałów, dotyczących tematyki detekcji i przeciwdziałania obecności niepożądanych bezzałogowych statków powietrznych.

W rozdziale pierwszym omówiono rys historyczny obejmujący rozwój technologii dronowych i genezę podjęcia tematu, wraz z nakreśleniem niebezpieczeństwa wynikającego z postępu w tej dziedzinie. Określono także główne cele pracy oraz sposób podejścia do rozwiązywania zaznaczonych problemów.

W rozdziale drugim przedstawiono wady i zalety różnych metod detekcyjnych oraz umotywowano wybór przyjętego podejścia. Porównano techniki oparte na sygnałach dźwiękowych, analizie obrazu, układach radarowych, rozpoznaniu radiowym oraz systemach mieszanych. Następnie przeprowadzono analizę rozwiązań, które stosowane są w przeciwdziałaniu sytuacjom niebezpiecznym wynikającym z użycia dronów. Przedstawiono ścieżki prawne i edukacyjne o charakterze systemowym, a także metody neutralizacji bezpośredniej. Umotywowano również wybór metody radioelektronicznej, będącej przedmiotem niniejszej pracy.

W rozdziale trzecim zarysowano podstawy teoretyczne dotyczące przetwarzania i analizy sygnałów w systemach cyfrowych, a w tym transformacji między dziedziną czasu i częstotliwości. Następnie opisano tor bezprzewodowej transmisji danych i scharakteryzowano środowisko propagacyjne fal radiowych. Wymieniono różne metody detekcji sygnałów, a osobną sekcję poświęcono wprowadzeniu do zagadnień sztucznej inteligencji w zastosowaniach związanych z kontekstem dysertacji. Rozdział zakończono opisem podstawowych technik w systemach zakłócania sygnałów radiowych.

W rozdziale czwartym wykonano przegląd rynku oraz metod kategoryzacji dronów z uwagi na rozmiar i masę urządzeń w kontekście potencjalnego zagrożenia. Dodatkowo, przeanalizowano zestaw sygnałów radiowych, które są wymagane do ich poprawnego działania, oraz fal własnych emitowanych przez te obiekty. Kolejne sekcje zawierają podzieloną na kategorie analizę literatury zarówno w dziedzinie detekcji, jak i neutralizacji komercyjnych statków bezzałogowych przy wykorzystaniu metody radioelektronicznej.

W rozdziale piątym opisano koncepcję radia definiowanego programowo, przedstawiono najpopularniejsze modele dostępne na rynku, a wybrany układ do budowy prototypu został zarysowany bardziej szczegółowo. Następnie pokazano ograniczenia, jakie generuje zastosowanie interfejsu szeregowego w urządzeniach tej klasy, oraz przedstawiono sposoby minimalizacji ich wpływu. W aspekcie toru odbiorczego zaproponowano przeniesienie obliczeń transformacji czasowo-częstotliwościowej do części sprzętowej, a w kontekście

toru nadawczego odtwarzanie predefiniowanego przebiegu. Dodatkowo, dla obu kierunków przepływu sygnału wprowadzono ulepszenia w oprogramowaniu dotyczące przyspieszenia przestrajania częstotliwości środkowej. Prezentowany prototyp, wraz z wprowadzonymi modyfikacjami, został poddany wstępnym badaniom zarówno w warunkach laboratoryjnych, jak i zbliżonych do rzeczywistych.

W rozdziale szóstym skupiono się na aspekcie detekcji sygnałów emitowanych przez bezzałogowe statki powietrzne. Na potrzeby badań symulacyjnych realizowanych za pomocą metody śledzenia promieni wybrano przykładowy obiekt infrastruktury krytycznej i określono moce sygnału docierającego do rozproszonych czujników, aby pokazać wyższą skuteczność tego podejścia w odniesieniu do detektora centralnego. Następnie opisano propozycje dwuetapowej analizy widma, zorientowaną na optymalizację procesu przetwarzania sygnałów w zależności od miejsca wykonywania obliczeń. W podejściu tym detekcja sygnału odbywa się w klasyczny sposób, poprzez progowanie energii, a do zadania klasyfikacji binarnej zastosowano różne metody uczenia maszynowego. Alternatywnie, przeprowadzono także eksperymenty, w których zadanie detekcji i klasyfikacji realizowane jest w jednym kroku przy pomocy głębokich sieci neuronowych.

W rozdziale siódmym skoncentrowano się na temacie przeciwdziałania komercyjnym statkom bezzałogowym przy pomocy emisji fal radiowych poprzez opracowany efektor. Przeprowadzono symulacje wyznaczające stosunki sygnałów zakłócających do użytecznych, przy podejściu do modelowego obiektu chronionego, aby oszacować możliwy do uzyskania zasięg pracy urządzenia. Powyższe rozważania rozdzielono na scenariusze, w których niezależnie zakłócają się sygnały nawigacji satelitarnej oraz te wykorzystywane do sterowania dronem. Dodatkowo dla obu tych kategorii transmisji przeprowadzono analizę potencjalnego wpływu zakłócania na odbiorniki, oraz zaprezentowano eksperymenty mające na celu potwierdzenie przydatności proponowanego prototypu w opisywanym zadaniu.

W rozdziale ósmym omówiono najważniejsze dokonania i przedstawiono wnioski z przeprowadzonych prac, oceniono stopień realizacji przyjętych celów oraz wytyczono kierunki dalszych badań.

Rozdział 2

Detekcja i przeciwdziałanie bezzałogowym statkom powietrznym

2.1 Metody detekcji

W literaturze przedstawiono liczne strategie wykrywania bezzałogowych statków powietrznych, oparte na różnych zjawiskach fizycznych. Naukowcy w swoich algorytmach wykorzystują dane dźwiękowe, wizyjne, radarowe, lidarowe oraz radiowe. Każda z indywidualnych metod charakteryzuje się użytecznością w konkretnych warunkach i jednocześnie posiada swoje ograniczenia. Dostępne na rynku komercyjnym układy heterogeniczne, wykorzystujące fuzję danych, starają się połączyć zalety każdej z technik podstawowych w jeden spójny, uniwersalny system.

2.1.1 Akustyczne

Pierwsza analizowana metoda polega na wykrywaniu charakterystycznego wzorca akustycznego generowanego przez elementy napędowe bezzałogowych statków powietrznych. Źródłem tego dźwięku są przede wszystkim śmigła, a jego parametry zależą od ilości i kształtu łopat oraz prędkości obrotowej układu. Podstawowym sensorem jest tu mikrofon, który w aranżacji matrycowej może uzyskać charakterystykę kierunkową lub dodatkowo umożliwić pozycjonowanie intruza.

Przetwarzanie sygnałów dźwiękowych, których częstotliwości mieszczą się w granicach kilkudziesięciu kiloherców, stanowi stosunkowo niewielkie obciążenie dla komponentów obliczeniowych. Interesującą skuteczność detekcji można osiągnąć już przy użyciu systemów wbudowanych [19]. Jak pokazują badania, zastosowanie zestawu siedmiu mikrofonów i analizy fazowej pozwala na detekcję kierunku lotu drona. Dodatkowo, rozróżnienie typu urządzenia jest możliwe w zasięgu do 300 m przy wykorzystaniu charakterystyki czasowo-częstotliwościowej [20]. Ciekawy kierunek badań stanowi również wykorzystanie światłowodowych czujników akustycznych do budowania rozległej sieci monitorowania

antydronowego [21].

Niezaprzeczalnym atutem tej metody jest jej pasywny elektromagnetycznie charakter, z drugiej jednak strony, ciągła rejestracja dźwięku może wiązać się z pewnymi komplikacjami natury prawnej. Niezależnie od typu czujnika i złożoności algorytmu, zastosowanie tej techniki będzie utrudnione w miejscach o dużym natężeniu hałasu, takich jak lotniska czy tereny miejskie. Nie bez znaczenia dla możliwości detekcyjnych pozostaje także wpływ wiatru, opadów atmosferycznych czy temperatury. Naturalnym jest również niezależne dążenie producentów dronów do minimalizacji sygatur akustycznych poprzez optymalizację układów napędowych w celu zapewnienia komfortu użytkowania. Można również wspomnieć o nieskuteczności tej metody w obliczu płatowców szybujących, jednakże nie są one tak popularne jak aparaty wirnikowe.

2.1.2 Wizyjne

Podejście wizyjne i analiza obrazu, od dawna obecne w systemach monitoringu, zostały również dostosowane do potrzeb detekcji bezzałogowych statków powietrznych. W kategorii tej stosowane są zarówno kamery operujące w zakresie światła widzialnego, jak i podczerwieni. Dla zwiększenia skuteczności detekcji stosuje się także fuzję danych z obu sensorów [22]. Zastosowanie metod uczenia maszynowego oraz technik sztucznej inteligencji pozwala natomiast na automatyczne odnalezienie drona w obserwowanym kadrze, odróżniając go od innych obiektów w tle. Unikalną cechą tej metody jest możliwość posłużenia się nagraniem wtargnięcia jako materiałem dowodowym w postępowaniu procesowym.

Zaawansowane przetwarzanie obrazów może stanowić poważne wyzwanie dla układów obliczeniowych, szczególnie gdy mamy do czynienia z danymi o wysokiej rozdzielczości. Dodatkowo, dla zapewnienia dookólnego zabezpieczenia terenu stosuje się zestawy kamer, co zwiększa wielkość strumienia danych do analizy. Biorąc pod uwagę powyższe aspekty, wciąż toczą się badania nad optymalizacją sieci neuronowych dla zastosowań antydronowych [23]. Zasięg wykrywania w tej technice mocno zależy od stosowanych układów optycznych, co znacząco przekłada się na zróżnicowanie kosztowe takich rozwiązań. Możemy tutaj mówić o granicy obszaru detekcji rzędu kilkuset metrów dla zestawów standardowych oraz nawet o 3 kilometrach po zastosowaniu zaawansowanego teleobiektywu [24]. Stosowanie dużych przybliżeń pozwala jednak na monitorowanie jedynie wycinka przestrzeni i wymaga zastosowania dodatkowych urządzeń pozycjonujących, co utrudnia śledzenie kilku obiektów jednocześnie.

Metoda ta, podobnie jak detekcja akustyczna, nie powoduje emisji fal elektromagnetycznych. Pozwala to na skalowanie wielkopowierzchniowe i rozmieszczanie sensorów w taki sposób, aby przeszkody terenowe nie ograniczały pola widzenia. Osobnym wyzwaniem w tym przypadku jest zapewnienie przepustowości sieci przesyłowej lub zastosowanie lokalnego przetwarzania danych. Przyczyną spadku efektywności tej techniki mogą być także

warunki pogodowe ograniczające widoczność oraz nietypowe kształty dronów, które nie występowały w treningowej bazie sygnatur.

2.1.3 Radarowe

Technika radarowa znana jest z początków XX wieku z kategorii monitorowania ruchu morskiego i lotnictwa załogowego. Podstawowa zasada jej działania opiera się na analizie fali elektromagnetycznej odbitej od powierzchni obiektu znajdującego się w zasięgu skanowania. Klasyczne radary wymagały znacznego dostosowania, aby uzyskać zadowalającą skuteczność w odniesieniu do małych obiektów poruszających się z niewielkimi prędkościami. Postęp technologiczny spowodował, iż obecnie pozostają one najskuteczniejszą, ale jednocześnie najbardziej kosztowną ze wszystkich metod detekcji komercyjnych bezzałogowych statków powietrznych.

Zasięg radarów aktywnych, oprócz ograniczeń propagacyjnych, zależy głównie od mocy wiązki sondującej emitowanej przez nadajnik. Może wynosić od kilku do kilkunastu kilometrów, zapewniając dookólne pokrycie terenu oraz możliwość wykrywania wielu obiektów jednocześnie [25]. Interesującą możliwością tego podejścia jest analiza charakterystycznych sygnatur odbicia fal od powierzchni wirujących łopat śmigieł napędowych, co pozwala na odróżnienie drona od ptaka o podobnym rozmiarze [26]. W przypadku rozwiązań z tej kategorii należy liczyć się jednak z wymogiem pozyskania specjalnych licencji na użytkowanie nadajników radiowych. Dodatkowo, radary aktywne, których zasięgi się pokrywają, mogą wzajemnie na siebie oddziaływać. Wyłączając kategorię komercyjnych bezzałogowych statków powietrznych, metoda ta może napotkać ograniczenia w zetknięciu z celowo przygotowanymi systemami wojskowymi o zmniejszonym RCS (ang. *Radar Cross-Section*) oraz jest wrażliwa na obce środki walki elektronicznej.

Radar pasywny nie generuje sygnałów sondujących, a określenie położenia i prędkości wykrytych obiektów odbywa się na zasadzie analizy odbić fal pochodzących zwykle od nadajników telekomunikacyjnych lub telewizyjnych [27]. W tym wypadku zasięgi zależne są od lokalnych źródeł sygnałów, ale ogromną zaletą podejścia jest możliwość praktycznie dowolnego multiplikowania sensorów. Niestety, oprócz bardzo skomplikowanych procesów obliczeniowych, do przeprowadzenia pozycjonowania obiektu wymagana jest także pewna wiedza o rozmieszczeniu źródeł sygnałów referencyjnych. Minimalizacja skutecznej powierzchni odbicia w konstrukcjach bezzałogowców o przeznaczeniu wojskowym ma w tym przypadku taki sam wpływ na zmniejszenie wykrywalności, co w przypadku podejścia aktywnego. Jednakże, z uwagi na znacznie bardziej skryte działanie układu pasywnego, zastosowanie środków walki elektronicznej jest w tym przypadku utrudnione.

2.1.4 Lidarowe

Skanery lidarowe do mapowania przestrzeni wykorzystują laserową wiązkę sondującą, a zasada ich działania opiera się również na zjawisku odbicia falowego. Efektem procesu skanowania jest stworzenie ogromnego zbioru punktów, którego akwizycja polega na pomiarze czasu przelotu impulsów świetlnych. Przy pomocy tej techniki możliwe jest również wykrywanie charakterystycznych wzorców ruchu obrotowego łopat śmigieł napędowych [28]. Lidar potrafi zapewnić znacznie większą rozdzielczość obrazowania niż radar, ale kosztem zasięgu, który wynosi jedynie do kilkuset metrów [29].

Warunki pogodowe, takie jak deszcz i mgła, mocno ograniczają skuteczność transmisji sygnałów świetlnych, co przekłada się na dokładność tej techniki. Do zapewnienia dookólnego pokrycia w lidarach stosuje się rotujące z dużą prędkością elementy optyki, które mogą być wrażliwe na uszkodzenia mechaniczne [30]. Emisja wiązki laserowej nie wymaga dodatkowej licencji, dopóki jest zgodna z regulacjami prawnymi dotyczącymi bezpiecznych limitów mocy. Planując monitorowanie większej przestrzeni, należy jednak zadbać o poprawne rozmieszczenie i dobór skanerów, aby urządzenia wzajemnie na siebie nie wpływały.

2.1.5 Radiowe

W tym podejściu proces detekcyjny opiera się na monitorowaniu widma radiowego w kontekście komunikacji bezprzewodowej pomiędzy dronem a operatorem. Technika ta jest całkowicie pasywna, co sprzyja budowie systemu z wieloma sensorami i dążeniu do ich rozproszenia powierzchniowego w celu przełamania ograniczeń propagacyjnych. Dodatkowo, pozwala to na śledzenie wielu obiektów jednocześnie, praktycznie niezależnie od warunków atmosferycznych czy pory dnia. Unikalną cechą tej metody jest możliwość wykrycia statku bezzałogowego po włączeniu, ale jeszcze przed startem oraz wskazania pozycji operatora. Osiągalne zasięgi wynoszą kilkaset metrów, przy zastosowaniu prostych anten o dookólnej charakterystyce, do nawet kilkunastu kilometrów za pomocą specjalistycznych anten kierunkowych.

Do wykrycia obecności i identyfikacji komercyjnego statku bezzałogowego można wykorzystać nawet proste urządzenie do skanowania sieci Wi-Fi (ang. *Wireless Fidelity*), jednak metoda ta jest ograniczona jedynie do dronów używających zgodnego ze standardem protokołu wymiany danych [31]. Badaczom udało się nawet zdekodować ramkę danych identyfikacyjnych, którą jeden ze znanych producentów transmitował bez użycia szyfrowania, prawdopodobnie na potrzeby własnych systemów monitorowania ruchu dronowego [32]. Bardziej zaawansowane podejście uwzględnia analizę warstwy fizycznej radiowego protokołu komunikacyjnego. W tym przypadku urządzeniem zbierającym dane może być oscyloskop [33], analizator widma [34] albo platforma radia programowalnego [35]. Dwa pierwsze urządzenia charakteryzują się wysoką klasą dokładności, aczkolwiek ich koszt

oraz przeznaczenie laboratoryjne sprzyjają bardziej wsparciu w rozwoju algorytmów niż zastosowaniu praktycznemu. Z tego powodu to właśnie radio definiowane programowo jest podstawą aktualnie prezentowanego projektu, a jego budowa będzie przybliżona w kolejnych rozdziałach rozprawy.

Na ograniczenie skuteczności i zasięgu działania metody radiowej spory wpływ ma środowisko o wysokim zagęszczeniu różnych nadajników. Podobnie, precyzyjna detekcja w obszarach o znacznej gęstości zaludnienia jest utrudniona z uwagi na liczne emisje o podobnej charakterystyce oraz ogólnie podniesiony poziom szumów odniesienia. Podejście to, niestety, jest całkowicie nieskuteczne w przypadku operacji, w których nie występuje kontrola operatora, a dron nie wysyła danych telemetrycznych, poruszając się po uprzednio zaprogramowanej trasie. Powyższy scenariusz nie występuje często w zastosowaniach komercyjnych i niesie poważne utrudnienia dla realizacji zadań wymagających reakcji w czasie rzeczywistym.

2.1.6 Heterogeniczne

Jak już wspomniano na początku rozdziału, żadna z analizowanych metod stosowanych samodzielnie nie daje pewności wykrycia niepożądanych statków bezzałogowych. Rozwój i doskonalenie każdej z technik są wciąż niezwykle istotne, jednakże osiągnięcie pełnej świadomości sytuacyjnej wymaga konstrukcji układów wielosensorowych. Poza badaniami nad indywidualnymi elementami w zainteresowaniu naukowców pozostaje także zagadnienie optymalizacji procesu fuzji danych. W literaturze możemy znaleźć więc na przykład zastosowanie rozszerzonego filtra Kalmana w połączeniu danych z lidarów i radarów [36]. W budowaniu systemów heterogenicznych wciąż jednak podstawą są elementy rozpoznania wizyjnego, często zestawione ze skanerami radiowymi [37] lub układami radarowymi [38], wspomagane technikami uczenia głębokiego. Komplet wszystkich trzech sensorów wymienionych powyżej stanowi kolejny krok w budowaniu rozwiązania wielopoziomowego i zapewnia dalszą minimalizację wskaźnika fałszywych detekcji [39]. Systemy heterogeniczne mogą być bardzo rozbudowane, a jednocześnie dostosowane do wymaganego scenariusza. Osiągają zatem najlepszą efektywność, jednak koszty w tym podejściu są zdecydowanie najwyższe.

2.2 Metody przeciwdziałania

Skuteczny proces detekcji stanowi dopiero pierwszy krok w obronie przed wtargnięciami bezzałogowych statków powietrznych w chroniony obszar. Metody przeciwdziałania takim sytuacjom możemy kategoryzować w różny sposób, ale na potrzeby tej rozprawy wyróżniono głównie podejście prawne, efektory kinetyczne, środki energii skierowanej oraz techniki radioelektroniczne. W tym momencie warto zauważyć, że jedyną powtarzającą

się technologią w aspekcie detekcji, jak i neutralizacji, jest kategoria radioelektroniczna. Należy podkreślić również, że dobór metody przeciwdziałania powinien być zawsze adekwatny do zaistniałego poziomu ryzyka, dlatego zróżnicowanie w klasie efektorów jest także istotną kwestią.

2.2.1 Prawne i administracyjne

Wciąż wiele incydentów z udziałem statków bezzałogowych to efekt niezamierzonego działania. Ważnym aspektem jest więc edukacja i popularyzacja wiedzy na temat potencjalnego niebezpieczeństwa, jakie niesie za sobą nieodpowiedzialne użytkowanie. Jednym z systemowych rozwiązań mogą być regulacje prawne, wymuszające na producentach komercyjnych dronów implementację ograniczeń w oprogramowaniu, które będą wpływać na zachowanie obiektu. Jednym z nich jest zastosowanie wirtualnych barier (ang. *geofencing*), które definiują obszary wyłączone z lotów na podstawie sygnałów nawigacji satelitarnej. Parametry takich stref zapisane są w oryginalnym oprogramowaniu urządzenia i uniemożliwiają operacje drona w miejscach o ograniczonym dostępie, takich jak lotniska [40].

Możliwe jest również wprowadzenie pewnych działań zapobiegawczych w postaci przewidywalnej reakcji komercyjnego statku bezzałogowego na określone sytuacje. Brak sygnału nawigacji satelitarnej lub zanik komunikacji bezprzewodowej z operatorem mogą wymuszać określone bezpieczne zachowanie, np. powolne lądowanie lub powrót do bazy. Kolejnym krokiem, który jest już w trakcie realizacji, jest nakaz wyposażania dronów w jednolity system radiowy informujący o położeniu podobny do transpondera lotniczego. Nie zapobiegnie to bezpośrednio niebezpiecznym sytuacjom, ale znacznie uprości aspekt monitorowania przestrzeni powietrznej [41]. W momencie rozpoczynania realizacji badań nad tematem niniejszej rozprawy regulacje prawne w tym zakresie dopiero się klarowały. Status realizacji tej inicjatywy oraz aspekty techniczne zostaną przybliżone w kolejnym rozdziale.

2.2.2 Kinetyczne

Do kategorii kinetycznych środków neutralizacji zaliczamy wszystkie metody, które w sposób fizyczny naruszają strukturę statku bezzałogowego. Możemy tu wymienić przede wszystkim środki balistyczne i rakietowe, znane w wojskowości z przeciwdziałania zagrożeniom ze strony lotnictwa załogowego. Zastosowanie powyższych metod nie zawsze jest adekwatne do stwarzanego zagrożenia, ponieważ koszty oraz ryzyko przeprowadzenia neutralizacji mogą być niewspółmiernie wysokie. Dodatkowo, niewielkie rozmiary statków bezzałogowych i loty na niskim pułapie mogą znacząco utrudnić ich stosowanie. Odpowiedzią na to są specjalne konstrukcje dronów przechwytyjących, których celem jest lot, pościg i kontakt fizyczny z intruzem w celu neutralizacji [42].

Sytuacja, w której mamy do czynienia z możliwością niekontrolowanego rozbicia ze-strzelonego statku bezzałogowego, sama w sobie może być niebezpieczna. Bezpośredni upadek urządzenia o masie jednego kilograma z wysokości 50 m stanowi już zagrożenie życia ludzkiego [43]. Doprowadziło to do poszukiwania metod ograniczających to ryzyko. Początkowo rozwijano nawet system szkoleń ptaków drapieżnych do polowania i odrzucania pochwyconych dronów w bezpiecznym miejscu [44]. Podobna idea została zastosowana w wielu efektorach kinetycznych wykorzystujących sieci do splątania elementów napędowych. Wyrzutnie takie mogą być częścią większego, zautomatyzowanego systemu, stanowić moduł manualny kontrolowany przez człowieka lub być elementem wyposażenia innych dronów [45].

2.2.3 Radiowe

Zasada działania metody radioelektronicznej opiera się na ingerencji w sygnały radiowe używane w bezzałogowych statkach powietrznych za pomocą intencjonalnie generowanych fal zakłócających. W kategorii tej pierwszym podejściem jest oddziaływanie na sygnały nawigacji satelitarnej wykorzystywane przez komercyjne drony do pozycjonowania w przestrzeni. Należy jednak pamiętać, że jest to działanie, które może mieć wpływ także na wiele innych systemów i narusza regulacje prawne o zasięgu globalnym. Możemy tu wyróżnić próbę oszukania aktualnej pozycji statku bezzałogowego poprzez nadawanie sygnałów zbliżonych do rzeczywistych (ang. *spoofing*) [46] lub ich odcięcie (ang. *jamming*), generując na przykład fale o znacznie większej mocy [47].

Wymuszenie zakłamania pozycji jest znacznie trudniejsze do zrealizowania pod względem obliczeniowym, z uwagi na potrzebę oszukania kilku niezależnych systemów satelitarnych jednocześnie. Często układy pozycjonowania dronów są dodatkowo uodpornione na takie próby poprzez zastosowanie algorytmów wspieranych danymi z czujników inercyjnych. Alternatywnie, atak może zostać skoncentrowany na układzie wejściowym odbiornika, poprzez zatkanie toru analogowego lub wpłynięcie na pętlę synchronizacji [48]. Sygnały generowane przez satelity nawigacyjne charakteryzują się bardzo niskim poziomem, gdy docierają do odbiorników, co czyni je podatnymi na powyższe formy oddziaływania, nawet przy użyciu bardzo tanich urządzeń [49].

Drugie podejście to ingerencja w elementy łączności służące do bezpośredniej kontroli lotu statku bezzałogowego przez operatora. Tutaj możemy wyróżnić sygnały sterujące, które zazwyczaj mają charakter wąskopasmowy i są definiowane w kierunku od operatora do drona, oraz sygnały zwrotne, zwykle o szerszym paśmie, zawierające oprócz danych telemetrycznych także strumień wideo [50]. Model powyższej komunikacji zostanie przedstawiony bardziej szczegółowo w kolejnych rozdziałach. Reakcją obiektu na zanik tych sygnałów może być wejście w tryb awaryjny, powrót do operatora lub zawis w oczekiwaniu na powrót komunikacji.

Skuteczność tych form przeciwdziałania zależy nie tylko od stosunku mocy sygnału zakłócającego do rzeczywistego, ale także od zastosowanej charakterystyki i pasma generowanej fali. Zależności te również zostaną przedstawione w następnych sekcjach. Uogólniając jednak, metoda radioelektroniczna może być skuteczna nawet przy braku bezpośredniej widoczności optycznej celu i działać równocześnie na wielu intruzów. Dodatkowo koszt podstawowego urządzenia zakłócającego jest stosunkowo niewielki, co sprzyja łączeniu tego rozwiązania z innymi metodami. Na przykład, chwilowo spowolniony obiekt w obliczu braku kontroli operatora czy sygnału nawigacji satelitarnej, spowodowanego zakłóceniami, będzie łatwiejszym celem dla środków neutralizacji kinetycznej.

2.2.4 Energetyczne

Strategia funkcjonowania broni energii skierowanej opiera się na oddziaływaniu na cel za pomocą skoncentrowanej wiązki fal elektromagnetycznych o dużej energii, aby dokonać uszkodzeń podzespołów elektronicznych. Cechą wspólną wszystkich rodzajów broni energetycznej jest bardzo duży koszt samego urządzenia, aczkolwiek brak wymogu fizycznej amunicji zwiększa opłacalność pojedynczego użycia [51]. Dodatkowo, metody te są bezgłośnie, nie generują wybuchów i ograniczają powstawanie odłamków własnych, jak ma to miejsce przy zastosowaniu środków kinetycznych. Należąca do tej kategorii broń laserowa, wywołująca skumulowane miejscowe efekty cieplne, może być precyzyjnie kierowana i używana do przeciwdziałania celom pojedynczym, jak i grupowym, pozostającym w bezpośrednim zasięgu widoczności [52]. Broń mikrofalowa natomiast oddziałuje na intruzów, wywołując niszczące prądy i napięcia, generując fale o mocy znacząco większej niż środki walki radioelektronicznej [53]. Promień rażenia jest tutaj natomiast znacznie większy i mniej precyzyjny niż w przypadku broni laserowej. Pozwala to na niszczenie wielu obiektów jednocześnie, ale może także powodować oddziaływanie w przestrzeni poza aktualnym celem.

Rozdział 3

Wprowadzenie do tematyki walki elektronicznej

3.1 Wstęp

Systemy elektroniczne odgrywają kluczową rolę zarówno w taktyce ofensywnej, jak i defensywnej we współczesnej, niezwykle dynamicznej przestrzeni operacyjnej. W latach 1899-1902 działania na tym polu zostały przeprowadzane w czasie wojny burskiej, podczas której po raz pierwszy zastosowano łączność bezprzewodową. Podczas I Wojny Światowej operacje w spektrum radiowym rozwijały się i koncentrowały na przechwytywaniu nieszyfrowanych komunikatów. W trakcie II Wojny Światowej urządzenia elektroniczne stały się powszechnym elementem zabezpieczenia operacji bojowych, a procesy te zyskały miano „wojny radioelektronicznej”. Ponieważ wykorzystywano bezpośrednio promieniowanie elektromagnetyczne pochodzące z radiowych urządzeń elektronicznych, miało to racjonalne uzasadnienie [54]. W kontekście przestrzeni elektromagnetycznej zaczęto nawet w pewnym momencie mówić o „czwartym wymiarze” wojny, w uzupełnieniu do aspektu lądowego, morskiego i powietrznego [55]. Dzisiaj Walka Elektroniczna (ang. *Electronic Warfare*, EW) może zostać określona w szerokim odniesieniu jako całokształt działań ukierunkowanych na detekcję i namierzanie systemów elektronicznych, zmierzających do zakłócenia bądź uniemożliwienia operacji przeciwnikowi. Pojęcie to jest często stosowane w węższej domenie, zamiennie z pojęciem Walki Radioelektronicznej (WRE), gdzie również mówimy o rozpoznaniu w dziedzinie widma radiowego oraz przeciwdziałaniu za pomocą własnych środków emisji elektromagnetycznej [56].

Rozpoznanie radioelektroniczne, znane również jako rozpoznanie sygnałowe (ang. *Signal Intelligence*, SIGINT), składa się z dwóch głównych obszarów. Rozpoznanie elektroniczne (ang. *Electronic Intelligence*, ELINT) obejmuje identyfikację promieniowania elektromagnetycznego, które zwykle jest związane z sygnałami radarowymi. Rozpoznanie radiowe (ang. *Communication Intelligence*, COMINT) natomiast ukierunkowane jest na identyfika-

cję środków łączności [57]. W prezentowanym opracowaniu, wyłączając analizę informacji zawartych w przekazie bezprzewodowym, skupiono się na parametrach sygnałów tych środków, przybliżając się do drugiej kategorii. Detekcja sygnałów radiowych to szerokie zagadnienie w dziedzinie telekomunikacji, łączące różne aspekty fizyki, inżynierii oraz informatyki. Wykorzystanie zaawansowanych algorytmów przetwarzania sygnałów i technik analizy danych umożliwia uzyskanie precyzyjnych informacji, co ma kluczowe znaczenie w kontekście systemów monitorowania.

Celem przeciwdziałania elektronicznego (ang. *Electronic Countermeasures*, ECM) jest natomiast prowadzenie operacji w celu ograniczenia efektywności działania systemów elektronicznych przeciwnika [57]. Przykładem akcji z tego obszaru może być wykorzystanie impulsu elektromagnetycznego o szerokim widmie oraz źródła energii skierowanej. W kontekście tej pracy jednak skupiono się na ataku elektronicznym (ang. *Electronic Attack*, EA) przy użyciu łatwo dostępnych komponentów i emisji fal radiowych znajdujących się w zakresie zbliżonym do sygnałów wykorzystywanych przez systemy bezzałogowe. Głównie zbadane zostaną aspekty zakłócania na poziomie warstwy fizycznej transmisji bezprzewodowej, powodujące brak dostępności łącza (ang. *Denial of Service*, DoS). Jest to podejście, które nie wymaga dokładnej znajomości protokołu, w przeciwieństwie do cyberataku, gdzie działania odbywają się bliżej warstwy danych.

3.2 Analiza i przetwarzanie sygnałów

Pojęcie sygnału, w rozumieniu niniejszego opracowania, opisuje proces zmienności w czasie pewnej wielkości fizycznej związanej z falą elektromagnetyczną. Analiza sygnałów ma na celu pozyskanie informacji w nich zawartych, a przetwarzanie sygnałów to transformowanie ich postaci [58]. Sygnał analogowy może być opisany ciągłą funkcją matematyczną przyjmującą dowolną wartość z zakresu swojej zmienności i jest określony w każdej chwili czasu. W sygnale cyfrowym natomiast dziedzina i zbiór wartości są dyskretne.

Sygnały analogowe są przekształcane do postaci cyfrowej za pomocą procedur próbkowania i kwantyzacji. Próbkowanie równomierne to proces, w którym odstępy czasu między zbieraniem kolejnych danych są równe. Odwrotności tych odstępów czasu określamy jako częstotliwość próbkowania. Kwantyzacja natomiast polega na przypisaniu do chwilowej amplitudy sygnału analogowego odpowiedniej wartości cyfrowej z dyskretnego zbioru. Jeśli spełnione zostaną odpowiednie kryteria, postać ciągła może zostać odtworzona bez utraty niesionej informacji.

Zmienność sygnałów w czasie, a dokładniej jej prędkość oraz intensywność, wprowadza możliwość pozyskania pewnej dodatkowej charakterystyki. Można ją uzyskać przez analizę w dziedzinie częstotliwości i wprowadzenie terminu widma sygnału [59]. Dziedzina czasu i dziedzina częstotliwości to alternatywne sposoby reprezentacji tych samych danych. Wzajemne relacje między tymi dziedzinami są oparte na matematycznym przekształceniu

Fouriera, które jest fundamentalnym narzędziem w analizie sygnałów. Operacja ta pozwala przedstawić sygnał jako sumę funkcji sinusoidalnych o różnych parametrach, uwidaczniając częstotliwości składowe w nim zawarte.

3.2.1 Ciągła transformacja Fouriera

Jeśli funkcja rzeczywista, określona na przedziale otwartym, spełnia warunki Dirichleta [58], to jest to warunek wystarczający, aby posiadała ona transformatę Fouriera (ang. *Fourier Transform*). Zakładając analogowy sygnał deterministyczny $x(t)$, proste przekształcenie Fouriera jest zdefiniowane jako 3.1:

$$X(\omega) = \int_{-\infty}^{+\infty} x(t)e^{-j\omega t} dt, \quad (3.1)$$

a odwrotne przekształcenie Fouriera można zapisać jako 3.2:

$$x(t) = \frac{1}{2\pi} \int_{-\infty}^{+\infty} X(\omega)e^{j\omega t} d\omega, \quad (3.2)$$

gdzie zmienna ω jest pulsacją powiązaną z częstotliwością f i okresem T poprzez zależność 3.3:

$$\omega = 2\pi f = \frac{2\pi}{T}. \quad (3.3)$$

Zapis przekształcenia 3.1 można przedstawić we współrzędnych biegunowych 3.4:

$$X(\omega) = |X(\omega)| e^{j\varphi(\omega)}, \quad (3.4)$$

gdzie $|X(\omega)|$ nazywamy widmem amplitudowym, a $\varphi(\omega)$ widmem fazowym sygnału. Dla $\omega \geq 0$ mają one wyraźną interpretację fizyczną określającą gęstość amplitudową i fazową składowych harmoniczných.

3.2.2 Dyskretna transformacja Fouriera

Rozważmy sytuację, w której, obserwując sygnał analogowy $x(t)$, próbkujemy go w stałym odstępach T_s w chwilach $t_0 = 0, t_1 = T_s, \dots, t_{N-1} = (N-1)T_s$, pobierając w zamkniętym przedziale $[0, T]$ skończoną liczbę próbek $N = T/T_s$. Proces próbkowania spełnia twierdzenie Nyquista (Kotelnikowa-Shannona), a zatem nastąpił z częstotliwością $1/T_s$, która jest co najmniej dwa razy większa od granicznej częstotliwości występującej w sygnale $x(t)$. Budujemy w ten sposób odpowiednik dyskretny $x[n]$ o skończonej liczbie elementów N , zakładając, że wartości próbek poza przedziałem $[0, N-1]$ są zerowe [59]. Proces wycięcia fragmentu analizowanego sygnału bez modyfikacji amplitudy próbek nazywamy zastosowaniem okna prostokątnego. Zależności 3.5 i 3.6 przedstawiają finalnie parę dyskretnych transformat Fouriera (ang. *Discrete Fourier Transform*, DFT) sygnału impulsowego $x[n]$:

$$X[k] = \sum_{n=0}^{N-1} x[n] e^{-2\pi j kn/N} \quad dla \quad k = 0, \dots, N-1, \quad (3.5)$$

$$x[n] = \frac{1}{N} \sum_{k=0}^{N-1} X[k] e^{2\pi j kn/N} \quad dla \quad n = 0, \dots, N-1. \quad (3.6)$$

Użycie DFT umożliwia zastąpienie obliczeń typu ciągłego przez mnożenie i sumowanie wartości dyskretnych. Wykonywanie kalkulacji wprost ze wzoru 3.5 wymaga jednak N^2 operacji. Istnieje algorytm, który optymalizuje obliczenia DFT, określany jako szybka transformacja Fouriera (ang. *Fast Fourier Transform*, FFT). Najpopularniejszą wersją FFT jest ta o podstawie 2, gdzie długość wektora próbek wejściowych jest potęgą dwójki, a złożoność obliczeniowa wynosi $N \log_2 N$ [58].

3.2.3 Krótkoczasowa transformacja Fouriera

Krótkoczasowa Transformacja Fouriera (ang. *short-time Fourier transform*, STFT) umożliwia analizę charakterystyki sygnału zarówno w dziedzinie czasu, jak i w dziedzinie częstotliwości. Blok próbek przeznaczony do analizy początkowo dzieli się na segmenty przez przesuwające się w czasie okno. Aby uniknąć gwałtownych zmian na końcach przedziałów, wektory wycinane przez okna czasowe mogą nachodzić na siebie, a zastosowana funkcja okna może wpływać na amplitudy sygnału w danej sekcji. Dla sygnału ciągłego STFT jest opisana zależnością 3.7:

$$X(t, \omega) = \int_{-\infty}^{+\infty} x(\tau) \gamma(\tau - t) e^{-j\omega\tau} d\tau, \quad (3.7)$$

gdzie podczas każdego przesunięcia czasowego t stosujemy funkcję okna $\gamma(\tau - t)$ wyśrodkowaną względem t , i obliczamy TF dla $x(\tau)\gamma(\tau - t)$ [58]. Równanie 3.7 uwzględniając dyskretyzację zarówno czasu, jak i częstotliwości, można zapisać dla sygnału o długości N w postaci:

$$X[n, k] = \sum_{m=0}^{N-1} x[n - m] \gamma[m] e^{-j2\pi mk/N}, \quad (3.8)$$

gdzie m to numer próbki okna, n jest daną próbką sygnału, a k dyskretną częstotliwością. Dodatkowo, jeśli długość sygnału spełnia zależność $N = 2^p$, gdzie p to pewna liczba naturalna, wtedy w obliczeniach można zastosować algorytm FFT. Kwadrat modułu krótkoczasowej transformacji Fouriera $|X[n, k]|^2$ nazywa się spektrogramem, który jest szeroko stosowaną metodą wizualizacji danych. Stały rozmiar okna jednak powoduje, że zwiększenie rozdzielczości czasowej pogarsza dokładność częstotliwościową i odwrotnie. Odpowiedni dobór tych parametrów zależy również od konkretnego zastosowania.

3.3 Tor komunikacyjny

Istotą każdego systemu bezprzewodowej wymiany danych jest przesyłanie informacji przez ośrodek propagacji fal radiowych. Jest to złożony proces, który zależy od wielu zjawisk, a ich opis wymaga zastosowania zaawansowanych modeli matematycznych i metod probabilistycznych. Elementarny tor komunikacyjny składa się z nadajnika, będącego źródłem sygnału o mocy P_t , anteny nadawczej o zysku G_t , anteny odbiorczej o zysku G_r i odbiornika, do którego dociera moc P_r . Pomiedzy nadajnikiem a odbiornikiem występuje radiowy kanał propagacyjny o tłumieniu L . Zjawisko to można opisać zależnością 3.9:

$$P_r = \frac{G_t G_r}{L} P_t, \quad (3.9)$$

gdzie moce P_r i P_t są wyrażone w watach. W obliczeniach związanych z aspektami radiowymi często jednak używa się jednostki pochodnej od bel'a jaką jest decybel, który jest miarą logarytmiczną oznaczaną jako dB. Korzysta się z niej zazwyczaj, gdy chcemy porównać wielkości zmieniające się w bardzo szerokim zakresie, a interesują nas zmiany względne danej wartości P odniesionej do P_0 . Można to zapisać jako 3.10:

$$P_{dB} = 10 \log_{10} \frac{P}{P_0}. \quad (3.10)$$

W pomiarach mocy sygnałów za wartość odniesienia P_0 przyjmuje się 1 mW, a używaną jednostką jest dBm. Przy określaniu zysku anteny natomiast poziom referencji stanowi wzmocnienie hipotetycznej anteny izotropowej wyrażone jako dBi. Korzystając z właściwości zapisu logarytmicznego, zależność 3.10 przedstawia się jako 3.11:

$$P_r = P_t + G_t + G_r - L. \quad (3.11)$$

Wyznaczenie współczynnika tłumienności L jest zadaniem wymagającym opisanie zjawisk związanych z rozpraszaniem, odbiciem czy dyfrakcją sygnału, ale jest ono kluczowe w kontekście określenia poziomu sygnału na wejściu odbiornika [60].

3.3.1 Radiowy kanał propagacyjny

Kanał propagacyjny to medium wpływające na amplitudy, fazy i opóźnienia składowych wielodrogowych pola elektromagnetycznego podczas rozchodzenia się fal radiowych pomiędzy anteną nadawczą a odbiorczą. Sygnał przechodzący przez ten kanał podlega zakłóceniom, które możemy podzielić na multiplikatywne oraz addytywne. Na składnik multiplikatywny wpływają zjawiska fizyczne, takie jak odbicie, absorpcja, rozpraszanie, dyfrakcja czy refrakcja. Ogólnie te zjawiska można zgrupować w pojęcie zanikania fali elektromagnetycznej, wśród których wyróżniamy tłumienie ścieżki (ang. *path loss*), przesłanianie

(ang. *shadowing*) i zaniki wielościeżkowe (ang. *multipath fading*) [61]. Składnik addytywny może pochodzić natomiast od efektów atmosferycznych, promieniowania kosmicznego, zakłóceń od sąsiednich nadajników, urządzeń elektrycznych czy samego odbiornika i szumów cieplnych elementów w nim zawartych.

Tłumienie ścieżki prowadzi do ogólnego spadku poziomu sygnału, a spowodowane jest głównie wzrostem dystansu między nadajnikiem a odbiornikiem. Fizyczne zjawiska, które mają wpływ na rozprzestrzenianie się fal elektromagnetycznych, to przeszkody w postaci drzew, budynków czy ukształtowania terenu. Tłumienie ścieżki zazwyczaj wyraża się w decybelach jako stosunek mocy nadawanej do odbieranej. Modelowanie propagacji, czyli przyjęcie pewnego wzoru matematycznego uwzględniającego częstotliwość, odległość czy wysokości anten, ma na celu zazwyczaj określenie zasięgu systemu radiowego. W kontekście tego opracowania posłuży także później do określenia odległości skutecznej detekcji dronowej oraz zasięgu neutralizacji. Podstawowym podejściem w tym temacie jest szacowanie tłumienia wolnej przestrzeni (ang. *Free Space Loss*, FSL) wyznaczane zgodnie z równaniem Friisa 3.12:

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d} \right)^2, \quad (3.12)$$

gdzie λ jest długością fali, d odległością między nadajnikiem a odbiornikiem, a pozostałe oznaczenia są zgodne z zależnością 3.9. Zakładając $G_t = G_r = 1$ tłumienie L dla modelu wolnej przestrzeni, możemy zapisać jako 3.13:

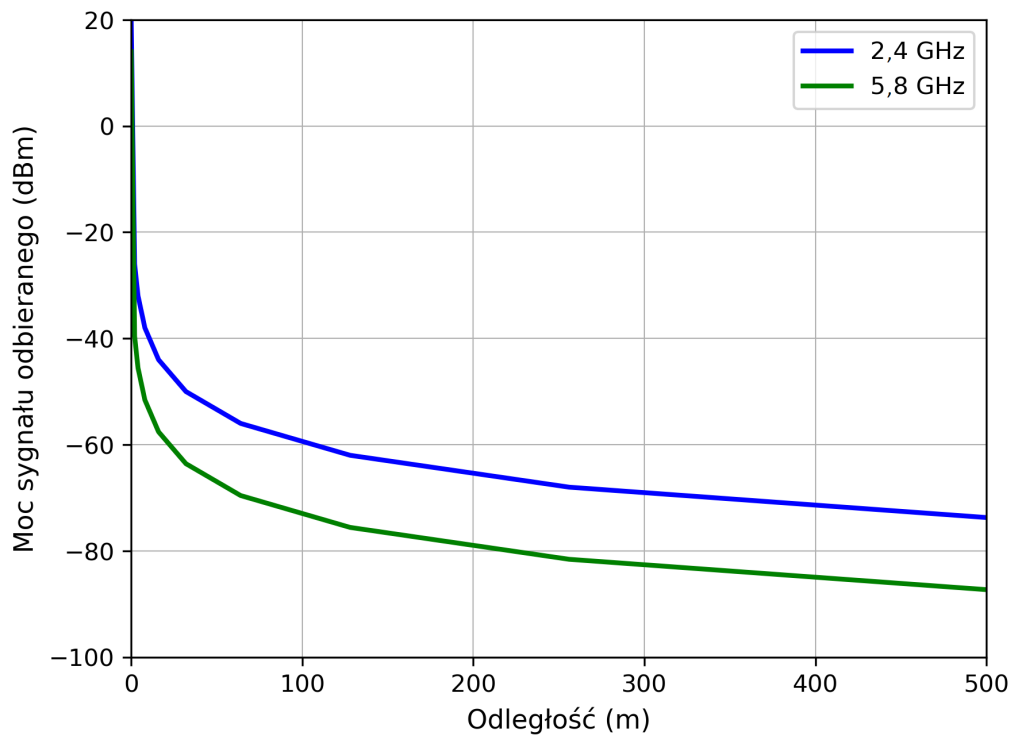
$$FSL = \frac{P_t}{P_r} = \left(\frac{4\pi d}{\lambda} \right)^2, \quad (3.13)$$

co przy podstawieniu $\lambda = \frac{c}{f}$ można przedstawić w skali decybelowej 3.14:

$$FSL_{dB} = 32,44 + 20 \log_{10} d_{km} + 20 \log_{10} f_{MHz}, \quad (3.14)$$

gdzie d oznacza odległość między antenami w kilometrach, a f częstotliwość w megahercach. Wartość ta często jest używana jako poziom odniesienia, gdyż w zdecydowanej większości przypadków tłumienie rzeczywiste jest jedynie większe. Przykładowe obliczenia poziomu sygnału w zależności od odległości, zakładając moce nadawania w danych pasmach zgodne z regulacjami obowiązującymi na rynku europejskim i przykładowym dronem, zaprezentowano na 3.1. W przypadkach, gdy dokładne modelowanie matematyczne nie jest możliwe, stosuje się podejście empiryczne, oparte na wynikach dużej kampanii pomiarowej. Jednym z najpopularniejszych w tej kategorii jest model Okumura-Hata, który przyjmuje różne parametry dla środowiska otwartego, zurbanizowanego lub podmiejskiego [61].

Zaniki dużej skali czy przesłanianie wynikają z dodatkowych zmian amplitud składowych sygnału, które nakładają się na tłumienie ścieżki opisane wcześniej. Zmiany te mogą być bardziej gwałtowne i wynikać zarówno z ruchu nadajnika, jak i ze zmienności otoczenia. Zaniki małej skali, czy zaniki szybkie, natomiast, spowodowane są bardzo małymi



Rysunek 3.1: Poziom sygnału w zależności od odległości przy założeniu modelu tłumienia wolnej przestrzeni. Dla częstotliwości 2,4 GHz przyjęto moc początkową 20 dBm, a dla częstotliwości 5,8 GHz moc początkowa to 14 dBm.

zmianami położenia anten i wpływają na zmiany faz poszczególnych składowych sygnału. Dodatkowo możemy tutaj wyróżnić kanał z zanikiem płaskim (ang. *flat fading*) lub selektywnym (ang. *selective fading*), gdy dla sygnałów szerokopasmowych pojawia się także zależność tłumienia od częstotliwości. Zjawiska te są często modelowane statystycznie przy użyciu funkcji gęstości prawdopodobieństwa. Dla przypadku dużej liczby odbić i braku bezpośredniej widoczności anten (ang. *Non Line-of-Sight*, NLOS) używa się dystrybucji Rayleigh'a, a kiedy ścieżka bezpośrednia dominuje (ang. *Line-of-Sight*, LOS) zastosowanie ma dystrybucja Rice'a [62].

3.3.2 Modelowanie kanału

Kanał AWGN (ang. *Additive White Gaussian Noise*) stanowi podstawowy model odniesienia w analizie wielu systemów komunikacyjnych. Sygnał propagujący się przez ten kanał dociera do odbiornika, pomniejszony o wartość tłumienia ścieżki i zniekształcony przez dodanie pewnej porcji szumu. W tym przypadku zakłada się dla uproszczenia sytuację stacjonarną oraz to, że sygnał jest wąskopasmowy, a tłumienie nie zmienia się w obrębie szerokości jego pasma. Charakterystyka zakłóceń jest addytywna, szum biały ma równomierną moc w całym paśmie, a rozkład Gaussa posiada zerową średnią wartość w dziedzinie czasu. Po przejściu przez kanał, szum posiada już skończoną moc i ograniczone

pasmo. Na wejściu odbiornika pojawia się więc sygnał, na który składają się komponent użyteczny i szum. Wyznaczając stosunek mocy sygnału użytecznego do szumu (ang. *Signal to Noise Ratio*, SNR) możemy określić jakość odbieranej transmisji i w ujęciu ogólnym wyrazić ją jako 3.15:

$$SNR = \frac{P_s}{P_n}, \quad (3.15)$$

gdzie P_s oznacza moc sygnału użytecznego, a P_n moc szumu. Jeżeli znane są wartości wariancji sygnału σ_s^2 i szumu σ_n^2 , to przy założeniu zerowej wartości średniej SNR możemy zapisać jako 3.16:

$$SNR = \frac{\sigma_s^2}{\sigma_n^2}. \quad (3.16)$$

Z uwagi na bardzo szeroki zakres dynamiczny, parametr SNR często wyrażany jest w skali decybelowej jako 3.17:

$$SNR_{dB} = 10 \log_{10} \frac{P_s}{P_n} = 10 \log_{10} \frac{\sigma_s^2}{\sigma_n^2}. \quad (3.17)$$

Znajomość parametru SNR w aspekcie komunikacji radiowej pozwala na osiągnięcie optymalnej wydajności transmisji, gdyż zgodnie z nim można na przykład dostosowywać metody kodowania i modulacji przesyłanego strumienia do pojemności kanału. W środowisku symulacyjnym, gdzie matematycznie potrafimy wygenerować zmodulowany czysty sygnał bez jakichkolwiek zakłóceń, nałożenie funkcji AWGN pozwala na precyzyjną kontrolę i uzyskanie pożądanego poziomu SNR w celach eksperymentalnych. W środowisku naturalnym natomiast estymacja tego parametru może być wspomagana danymi za pomocą specjalnych symboli pilotów lub znanych sekwencji treningowych wstawionych do strumienia danych. W przypadku braku wcześniejszej informacji o strukturze sygnału estymacja SNR musi przebiegać w inny sposób [63]. Procesy wyznaczania SNR mogą być realizowane zarówno w dziedzinie czasu, jak i częstotliwości, różnić się w zależności od przyjętego kanału czy metody modulacji, a także wymagać dodatkowej korekty przy bardzo niskich wartościach parametru [64].

3.4 Detekcja sygnałów radiowych

Podjęcia do detekcji sygnałów radiowych są różnorodne, a wybór optymalnego zależy od specyfiki problemu oraz dostępnych zasobów obliczeniowych. Rozpatrując tylko pojedynczy węzeł detekcyjny, możemy go podzielić, biorąc pod uwagę zakres rozpoznania, na metody wąskopasmowe oraz szerokopasmowe. Techniki wąskopasmowe stosuje się do analizy pojedynczego zakresu częstotliwości, a podstawowe warianty w tym podejściu to: detekcja energii, analiza cyklostacjonarna i aplikacja filtrów dopasowanych [65]. W podejściu szerokopasmowym można stosować dedykowane metody lub skorzystać z technik

wąskopasmowych, skanując widmo w sposób sekwencyjny [66]. W zastosowaniach polegających na poszukiwaniu okazjonalnego okna transmisyjnego podejście szeregowie może okazać się zbyt wolne. W przyjętym scenariuszu, gdzie celem jest detekcja obecności nadajnika i jego identyfikacja, spełni ono jednak swoje zadanie wystarczająco dobrze, stąd w kolejnych sekcjach skupiono się na metodach z tej kategorii.

Detekcja sygnału w ujęciu ogólnym może sprowadzić się do wyboru pomiędzy dwoma hipotezami 3.18:

$$\theta = \begin{cases} H_0 : y[n] = w[n] \\ H_1 : y[n] = s[n] + w[n] \end{cases} \quad (3.18)$$

gdzie $n = 1, \dots, N$ jest numerem kolejnej próbki, $y[n]$ jest sygnałem docierającym do detektora, a $w[n]$ stanowi AWGN. Decyzja θ przybiera stan H_1 , gdy w badanej próbce wykryto obecność sygnału lub H_0 w przeciwnym przypadku. Dla oceny jakości pracy detektora możemy zdefiniować następujące metryki:

$$P_D = Pr(H_1|H_1), \quad (3.19)$$

$$P_{FA} = Pr(H_1|H_0), \quad (3.20)$$

$$P_M = Pr(H_0|H_1), \quad (3.21)$$

$$P_{CD} = Pr(H_0|H_0) + Pr(H_1|H_1). \quad (3.22)$$

Prawdopodobieństwo detekcji P_D 3.19 określa stan, w którym transmisja została wykryta i jest ona rzeczywiście obecna. Prawdopodobieństwo fałszywego alarmu P_{FA} 3.20 określa natomiast sytuację, gdy detektor wykrywa sygnał, a w istocie nie jest on obecny. Prawdopodobieństwo pominięcia detekcji P_M 3.21 opisuje sytuację, w której przegapiono obecność transmisji. Prawdopodobieństwo poprawnej decyzji P_{CD} 3.22 określa szansę, że wynik pomiaru odpowiada rzeczywistej obecności lub brakowi sygnału. Idealny scenariusz wskazujący na optymalne zachowanie detektora zakłada osiągnięcie zarówno bardzo niskiego prawdopodobieństwa fałszywego alarmu, jak i wysokiego prawdopodobieństwa wykrycia. Jednak w praktyce konieczne jest oszacowanie, czy prawdopodobieństwo wykrycia osiągnęło wystarczająco wysoki poziom, przy założeniu stałego prawdopodobieństwa fałszywego alarmu.

3.4.1 Detekcja energii

Pierwsza metoda analizy obecności sygnałów radiowych to detekcja energii, której wykorzystanie nie wymaga wiedzy o charakterystyce poszukiwanego sygnału [67]. Znajduje ona zastosowanie w systemach radarowych oraz w koncepcji radia kognitywnego, a stosowana może być zarówno w dziedzinie czasu, jak i częstotliwości. W podejściu tym binarna decyzja o występowaniu transmisji podejmowana jest na zasadzie porównania

sygnału z progiem decyzyjnym (ang. *threshold*). Zakładając zapis odebranego sygnału w postaci dyskretnej jako 3.23:

$$y[n] = s[n] + w[n], \quad (3.23)$$

gdzie $s[n]$ określa kolejne próbki sygnału, $w[n]$ to szum, a n jest indeksem próbki, to statystyka testowa dla wektora o rozmiarze N może zostać przedstawiona jako 3.24:

$$E = \frac{1}{N} \sum_{n=0}^{N-1} |y[n]|^2. \quad (3.24)$$

Proces detekcji, w którym λ stanowi wartość progową, można wtedy zapisać jako 3.25:

$$\theta = \begin{cases} H_1 & \text{dla } E \geq \lambda \\ H_0 & \text{dla } E < \lambda \end{cases}. \quad (3.25)$$

Decyzja θ przybiera stan H_1 , gdy w badanej próbce wykryto obecność sygnału lub H_0 w przeciwnym przypadku. Dobór odpowiedniej wartości progowej jest tutaj najtrudniejszym zadaniem, którego realizacja powinna polegać na zapewnieniu odpowiedniego stosunku prawdopodobieństwa detekcji do fałszywego alarmu. W przypadku detekcji energii P_D i P_{FA} można zapisać odpowiednio jako 3.26 oraz 3.27:

$$P_D = Pr(E > \lambda | H_1), \quad (3.26)$$

$$P_{FA} = Pr(E > \lambda | H_0). \quad (3.27)$$

Niewątpliwym atutem tej metody jest niska złożoność obliczeniowa oraz szeroka możliwość zastosowania. Zależna jest ona jednak mocno od zakłóceń wewnątrz-pasmowych (ang. *in-band interference*), szczególnie przy analizie w dziedzinie czasu. Trudności w estymacji mocy szumu oraz jego zmienności są dodatkowym aspektem wpływającym na spadek skuteczności tej techniki w złożonym środowisku elektromagnetycznym. Aby zminimalizować te wady, w pierwszym kroku można zaproponować dynamiczne przydzielanie wartości progowej. Opracowań w tym temacie jest bardzo wiele, a proponowane algorytmy często zawierają zmienne dobierane empirycznie. Autorzy w [68] zaproponowali jednak metodę automatyczną, nie wymagającą strojenia, a także przedstawili niezależny sposób na wykrycie, czy w badanym zbiorze próbki zawierają tylko szum. Pozwoliło to na osiągnięcie prawdopodobieństwa fałszywego alarmu poniżej poziomu 2% oraz na uproszczenie obliczeń, przy braku konieczności tworzenia histogramu, jak w innych metodach bazujących na algorytmie binaryzacji Otsu [69]. Kolejną techniką jest zastosowanie dwóch wartości progowych, w której zakłada się wykrycie sygnału, gdy próbka badana znajduje się powyżej górnego progu, a jego brak w przypadku, gdy jest ona poniżej progu dolnego [70]. W strefie

między progami decyzja nie będzie podejmowana, co w szczególnych przypadkach może spowodować duże opóźnienie detektora. Aby tego uniknąć, w strefie niepewności można użyć uśrednionych wartości historycznych lub zastosować metodę progu pojedynczego [71]. Stosując to podejście, udało się utrzymać prawdopodobieństwo detekcji powyżej poziomu 90%, nawet przy SNR równym -15 dB.

3.4.2 Detekcja oparta na cechach charakterystycznych

W podejściu do detekcji wykorzystuje się właściwości statystyczne sygnałów, takie jak współczynnik korelacji i kowariancji. Wyróżnikiem rozwiązań z tej kategorii jest możliwość odróżnienia sygnału zmodulowanego od zakłóceń, które zazwyczaj mają w szerokim zakresie charakter stacjonarny [72].

W systemach komunikacji bezprzewodowej ramki danych uzupełniane są o znane wzorce, które mogą służyć do synchronizacji nadajnika i odbiornika lub do modelowania kanału. Wzorce te mogą tworzyć preambułę ramki (ang. *preamble*), znajdować się w okolicy jej środka (ang. *mid-amble*) lub przyjmować formę regularnie transmitowanych znanych pilotów. Mając wiedzę o charakterze tego sygnału, można przeprowadzić proces autokorelacji ramki radiowej z odpowiednio opóźnioną jej kopią. Współczynnik korelacji przyjmie wartość maksymalną w momencie, kiedy okno pomiarowe znanego wzorca pokryje się z jego przesuniętą w czasie kopią, a przy braku sygnału użytecznego utrzymywał będzie natomiast wartość bliską zeru [73]. Podejście to pozwala na osiągnięcie lepszych wyników niż przy detekcji energii, wymaga jednak już znacznej wiedzy o poszukiwanym sygnale [74].

Macierz kowariancji oraz rozkład według wartości osobliwych (ang. *Singular Value Decomposition*, SVD) również mogą być wykorzystane do detekcji sygnałów. Wyliczenie maksymalnych i minimalnych wartości własnych (ang. *eigenvalues*), a następnie porównanie ich stosunku z wartością progową, służy jako wyznacznik przy podejmowaniu decyzji o obecności sygnału [66]. Metoda ta również pozwala na osiągnięcie lepszych wyników niż detekcja energii, nie wymagając wcześniejszej wiedzy o strukturze sygnału, jednak złożoność obliczeniowa utrudnia jej użycie w czasie rzeczywistym [75].

Analiza cyklostacjonarna znajduje zastosowanie w procesie detekcji, z uwagi na okresowy charakter sygnałów generowanych przez układy radiowe [76]. Parametry statystyczne, takie jak wartość średnia, wariancja czy współczynnik autokorelacji, pozwalają na odróżnienie intencjonalnej transmisji od szumu stacjonarnego. Techniki cyklostacjonarne zapewniają lepszą wydajność wykrywania niż detekcja energii, są mniej podatne na niepewność szumu oraz pozwalają na zmniejszenie prawdopodobieństwa fałszywego alarmu [73]. Aby osiągnąć jednak dużą skuteczność w tym podejściu, czas zbierania danych do analizy musi zostać znacząco wydłużony [66].

Zastosowanie filtra dopasowanego uważane jest za jedną z najbardziej skutecznych metod detekcji, pod warunkiem posiadania pełnej wiedzy o parametrach transmisji. Znajac

wyznaczniki takie jak pasmo, częstotliwość i format ramki radiowej, urządzenie odbiorcze wyposażone w synchronizację nośnej jest w stanie porównać przychodzący sygnał z predefiniowanym wzorcem [77]. Główną zaletą tej metody to krótki czas pozyskiwania danych, niezbędny do zapewnienia pożądanej minimalizacji poziomu prawdopodobieństwa fałszywego alarmu. Wraz ze wzrostem liczby poszukiwanych sygnałów, zastosowanie filtra będzie coraz bardziej złożone oraz wpłynie na niezbędny wydatek energetyczny [73].

3.4.3 Detekcja oparta na entropii

Entropia to miara służąca do wyznaczenia stopnia nieokreśloności badanych stanów lub rozkładów zmiennych losowych [78]. Pojęcie to do teorii informacji wprowadził Claude Shannon w 1948 roku, a od tego czasu powstało wiele uogólnionych wariantów tej miary. Histogram, jako sposób prezentacji rozkładu cechy ilościowej, może zostać użyty także przy kalkulacji entropii [79]. Różne poziomy energii odbieranego sygnału przypisywane są do poszczególnych klas histogramu, a finalną decyzję o obecności sygnału podejmuje się poprzez porównanie z wartością progową. Entropię Shannona [80] możemy zapisać jako 3.28:

$$E_s = - \sum_{i=1}^L p_i \log_2(p_i), \quad (3.28)$$

gdzie L jest liczbą klas, a p_i określa częstotliwość wystąpień i -tej klasy. Entropię Rényi'ego natomiast jako 3.29:

$$E_1 = \frac{1}{1 - \alpha} \log_2 \left(\sum_{i=1}^L p_i^\alpha \right), \quad (3.29)$$

gdzie dodatkowy parametr α oznacza stopień entropii.

Jako że nieokreśloność szumu jest większa od nieokreśloności sygnału użytecznego, wyznacznik ten można stosować przy detekcji zarówno w dziedzinie czasu, jak i częstotliwości. W dziedzinie czasu jednak sygnał o niskim SNR rozprasza się wśród szumu, dlatego skuteczność detektora w tej domenie nie jest zadowalająca. Transformacja do dziedziny częstotliwości pozwala na uzyskanie lepszych wyników dla tej metody w stosunku do detektora energii, jak i do analizy cyklostacjonarnej [81]. Dodatkowo wykazano, iż podejście to zachowuje wysoką skuteczność nie tylko dla kanału AWGN, ale także dla modeli Rice'a i Rayleigh'a [82]. Badania porównawcze czterech różnych wariantów tej miary wykazały, że zastosowanie entropii Rényi'ego w porównaniu do entropii Shannona pozwala z tym samym prawdopodobieństwem detekcji wykryć sygnał przy SNR niższym o 11 dB dla kanału AWGN [83]. Biorąc pod uwagę konkretny przykład sygnału zmodulowanego oraz model kanału Rice'a, przewaga ta maleje do 3 dB [84]. Porównując w podobny sposób detektor energii z metodą entropii Rényi'ego w warunkach symulacyjnych, uzyskuje on przewagę rzędu 8 dB zarówno dla kanałów AWGN, jak i modelu Rayleigh'a [85]. Dodatkowe eksperymenty w środowisku rzeczywistym pokazały, że przy

założeniu prawdopodobieństwa detekcji na poziomie 90%, dla podejścia bazującego na entropii wyniki spadają o 3 dB w stosunku do symulacji.

Interesującym podejściem są także badania, które przedstawiają kaskadowe połączenie techniki opartej na energii i entropii [83]. Detektor energii działający w dziedzinie czasu został użyty jako wejściowy stopień wykrywania zgrubnego. W momencie braku wykrycia sygnału przez stopień pierwszy następuje transformacja do dziedziny częstotliwości oraz zastosowanie entropii Rényi'ego jako stopnia dokładnego. Metoda ta, dla założonego SNR -23 dB, osiągnęła prawdopodobieństwo detekcji na poziomie 63%, gdzie pojedyncze detektory wykazywały odpowiednio wartości 54% dla stopnia dokładnego oraz 21% dla stopnia zgrubnego.

3.5 Sztuczna inteligencja w systemach rozpoznania radiowego

Sztuczna inteligencja to temat, który na dobre zagościł zarówno w opracowaniach naukowych, jak i w życiu codziennym. Jej popularność związana jest z łatwym dostępem do narzędzi oraz, w pewnych kwestiach, prostotą uzyskania pożądanego efektu przy niewielkim nakładzie pracy. Grono entuzjastów tej dziedziny rośnie, gdyż pojawiające się ciągle nowe aplikacje wpływają wręcz rewolucyjnie na wiele praktycznych zastosowań. Z drugiej strony, nie brakuje również sceptyków, którzy nie wyolbrzymiają tych możliwości, zaznaczając wciąż, że to człowiek i jego doświadczenie są niezastąpione. Niezależnie od przyjmowanego stanowiska, warto jednak poznać ten temat oraz jego możliwości w kontekście systemów związanych z walką elektroniczną.

Wiele pojęć kojarzonych z tym tematem jest często używanych zamiennie, a nawet błędnie. Najszerszym określeniem jest tutaj sztuczna inteligencja (ang. *Artificial Intelligence*, AI), będąca zbiorem, do którego należą zarówno metody uczenia maszynowego (ang. *Machine Learning*, ML), jak i symboliczna sztuczna inteligencja [86]. Rozróżnienie tych dwóch terminów leży w podejściu do wykonania zadania. W rozwiązaniach symbolicznych określa się zasady i algorytm podejmowania decyzji, a w uczeniu maszynowym dostarcza się danych, a algorytm ma za zadanie wypracowanie reguł. Podzbiorem metod uczenia maszynowego jest dodatkowo uczenie głębokie (ang. *Deep Learning*, DL), w którym zazwyczaj wymaga się większych zbiorów danych treningowych oraz bardziej złożonych obliczeń. W podejściu tym algorytmy mogą poprawiać swoje wyniki w kolejnych iteracjach, bez znacznej ingerencji człowieka, jak ma to miejsce w innych metodach z tej podkategorii.

Podział metod uczenia maszynowego może być wykonywany na różne sposoby, a do głównych możemy zaliczyć przede wszystkim uczenie nadzorowane oraz nienadzorowane. Pierwsze z wymienionych podejść, wykorzystywane w niniejszej pracy, charakteryzuje się procesem nauki opartym na zbiorze danych wejściowych i wyjściowych o znanej wzajem-

nej relacji. Celem takiego działania jest wypracowanie uogólnionego pomysłu na to, aby wprowadzenie nowych danych wejściowych skutkowało odpowiednio przewidywalnym rezultatem. Dwa główne zastosowania uczenia nadzorowanego to rozwiązywanie problemu regresji, czyli prognozowanie pewnej wartości, oraz zagadnienie klasyfikacji, czyli przypisanie danej wejściowej do odpowiedniej kategorii. W uczeniu nienadzorowanym natomiast dane wejściowe nie posiadają etykiet, a to do zadania algorytmu należy znalezienie powiązań między nimi. Trzecim nurtem jest uczenie przez wzmacnianie, w którym, w przeciwieństwie do wcześniej wymienionych metod, nie przygotowuje się zestawu danych uczących, a środowisko do automatycznego ich zbierania [87].

3.5.1 Klasyczne i głębokie uczenie maszynowe

Zagadnienie detekcji w zakresie widma radiowego może być również traktowane jako problem klasyfikacji. Tradycyjne podejście, czyli takie sprzed rewolucji związanej z technikami głębokimi, oparte jest na sprecyzowanych modelach matematycznych i bazuje głównie na metodach statystycznych. Do najpopularniejszych w tym zakresie należą algorytm k najbliższych sąsiadów (ang. *K-Nearest Neighbours*, KNN), naiwny klasyfikator Bayesa (ang. *Naive Bayes*, NB), drzewa decyzyjne (ang. *Decision Trees*, TD) oraz lasy losowe (ang. *Random Decision Forests*, RDF). W koncepcji maszyn wektorów nośnych (ang. *Support Vector Machines*, SVM) budowana jest pewna przestrzeń decyzyjna, a celem jej działania jest wyznaczenie hiperpłaszczyzny separującej obiekty należące do dwóch różnych klas [86].

Kolejną techniką są sztuczne sieci neuronowe (ang. *Artificial Neural Networks*, ANN), czyli algorytmy uczące się, które próbują naśladować funkcje biologicznego mózgu. Sieć neuronowa zbudowana jest z pojedynczych, połączonych ze sobą elementów zestawionych w warstwy. Każdy element posiada zestaw sygnałów wejściowych, scharakteryzowanych przez wagi i pojedyncze wyjście. Architekturę sieci można zdefiniować poprzez podanie systemu połączeń między warstwami, reguły modyfikacji wag w procesie uczenia oraz funkcji aktywacji elementu.

Pierwszy model neuronu, który mógł modelować proste funkcje logiczne, pojawił się już w 1943 roku. Frank Rosenblatt wykorzystał ten model do zaproponowania pierwszej prostej sieci neuronowej, znanej jako perceptron, w 1958 roku. Wygaszenie entuzjazmu związanego z tą technologią miało miejsce w 1969 roku po publikacji, w której udowodniono niezdolność sieci jednowarstwowej do obliczeń funkcji logicznej XOR. Dopiero w 1986 roku, po przedstawieniu algorytmu wstecznej propagacji błędów, pozwalającego uczyć sieci wielowarstwowe, rozpoczęła się druga rewolucja związana ze sztucznymi sieciami neuronowymi. Kilkanaście lat później ANN stały się dobrze znaną i ustabilizowaną technologią, a ich możliwości były limitowane mocą obliczeniową systemów komputerowych. Kolejny przełom, częściowo związany z pojawieniem się wydajnych elementów obliczenio-

wych, jakimi są karty graficzne, rozpoczął się około roku 2006 wraz z pojawieniem się sieci głębokich (ang. *Deep Neural Network*, DNN). Często zawierają one wyspecjalizowane warstwy neuronów związane z konkretnym typem danych oraz łączą się w wielostopniowe struktury, wciąż jednak wykorzystując perceptrony i metody wstecznej propagacji błędów. Przetwarzanie złożonych zbiorów danych w niestrukturyzowanej postaci zostało zdominowane przez pojawienie się tej nowej dziedziny, ale fenomen tego podejścia leży w ilości, a nie w jakości danych, na których następuje proces trenowania [88].

3.5.2 Topologie wybranych sieci neuronowych

Najprostszy element decyzyjny, jakim jest perceptron, może służyć do budowy regularnych, większych struktur. Natomiast bardziej zaawansowany perceptron wielowarstwowy składa się z osobnej warstwy wejściowej i wyjściowej, a pomiędzy znajdują się dodatkowo warstwy ukryte. Połączenia między nimi są skierowane od wejścia, przez warstwy ukryte do wyjścia, bez połączeń zwrotnych, co jest wyznacznikiem architektury jednokierunkowej (ang. *Feedforward Network*). Warstwa wejściowa stanowi interfejs do świata zewnętrznego i zależna jest od rozmiaru danych, a warstwa wyjściowa to miejsce zbierania cech i wypracowania odpowiedzi sieci. Od budowy warstw wewnętrznych zależy zdolność sieci do wykrywania tych cech i kategoryzacji sygnałów. Zbyt duża liczba warstw ukrytych lub neuronów w tych warstwach może ograniczyć zdolność modelu do generalizacji problemu. Tendencję tę nazywa się przeuczeniem (ang. *overfitting*), a w przypadku sieci zbyt małej może wystąpić niedouczenie (ang. *underfitting*) [88].

Sieci rekurencyjne (ang. *Recurrent Neural Networks*, RNN) oparte są na warstwach jednokierunkowych typu perceptronowego, ale ich kluczowe elementy to dodatkowe sprzężenia zwrotne, umożliwiające przetwarzanie informacji z poprzednich kroków procesu. Mechanizm pętli wyprowadzany jest z warstwy ukrytej bądź z warstwy wyjściowej w celu uzyskania efektu pamięci o stanach wcześniejszych i zbudowania szerszego kontekstu. Podczas trenowania tych struktur mogą wystąpić jednak swoiste problemy ze zanikającym i eksplodującym gradientem. W ramach rozwiązania tego zagadnienia opracowany został wariant sieci o długiej pamięci krótkotrwałej (ang. *Long Short-Term Memory*, LSTM), wprowadzający mechanizm bramkowania regulującego przepływ informacji między komórkami. Dzięki zdolności do zapamiętywania długoterminowych zależności, topologie te są używane w rozpoznawaniu mowy, pracy z tekstem czy analizie szeregów czasowych [87].

Sieci konwolucyjne (ang. *Convolutional Neural Network*, CNN), których nazwa pochodzi od operacji splotu, czyli konwolucji, są jednym z najpopularniejszych modeli stosowanych do zadań związanych z przetwarzaniem obrazów. Pierwowzorem dla nich był neocognitron, opracowany w 1980 roku, a pierwsza sieć splotowa została zaproponowana w 1998 roku. Od tego czasu zagadnienia związane z tym modelem dalej rozwijały się pod nazwą uczenia głębokiego, a same sieci wielowarstwowe tego typu zaczęto nazywać sieciami głębokimi.

Liczba neuronów konwolucyjnych oraz wielkość maski ustalane są na etapie tworzenia architektury sieci przez użytkownika. Przemieszczająca się po obrazie maska stanowi pewnego rodzaju filtr, który poprzez wykonywane operacje wprowadza zbędną nadmiarowość, zwiększając dodatkowo złożoność obliczeniową. Aby ograniczyć to zjawisko, w kolejnym kroku następuje operacja łączenia sąsiednich wyników poprzez zastosowanie pośrednich warstw próbkujących (ang. *pooling layer*). Mają one za zadanie zmniejszyć wymiarowość problemu poprzez uśrednienie (ang. *average pooling*) lub znalezienie maksimum (ang. *max pooling*) w analizowanym obszarze, co skutkuje uogólnieniem informacji dotyczących danej cechy. Następnie macierze wynikowe ostatniej warstwy konwolucyjnej przekształcane są do zapisu wektorowego operacją spłaszczenia (ang. *flatten*) i mogą przechodzić do kolejnych warstw w pełni połączonych typu perceptron wielowarstwowy [88].

3.5.3 Ocena i porównywanie modeli

Ocena właściwości modelu w celu określenia jego jakości i momentu zakończenia procesu uczenia wymaga zastosowania pewnego kryterium liczbowego. Miary sukcesu to wskaźniki, które mogą być odmienne dla różnych zadań uczenia maszynowego, a najczęściej mierzą poziom błędów popełnianych przez wytrenowany model. W czynnościach związanych z regresją najczęściej preferowany jest błąd średniokwadratowy (ang. *Mean Square Error*, MSE), za pomocą którego określa się, jak blisko znajdują się prognozy od rzeczywistych wartości 3.30:

$$MSE = \frac{1}{N} \sum_{i=1}^N (X_i - \hat{X}_i)^2, \quad (3.30)$$

gdzie X_i jest wartością obserwowaną, $\hat{X}_i$ wartością przewidywaną, a N określa liczbę punktów danych.

W zagadnieniu klasyfikacji natomiast miara trafności może zostać zapisana jako 3.31:

$$N_{ov} = \frac{n_T}{n}, \quad (3.31)$$

gdzie n_T to liczba poprawnie sklasyfikowanych przykładów testowych, a n jest wielkością zbioru. Dodatkowo łączny błąd klasyfikacji może być przedstawiony jako 3.32:

$$E_{ov} = 1 - N_{ov} = \frac{n_F}{n}, \quad (3.32)$$

gdzie n_F stanowi liczbę błędnie sklasyfikowanych przykładów testowych [86]. Do szczegółowej analizy wyników pracy modelu można zastosować dwuwymiarową macierz pomyłek (ang. *confusion matrix*), która w sposób tabelaryczny podsumowuje wyniki klasyfikacji. Każda kolumna w tej macierzy przedstawia możliwe rzeczywiste wartości atrybutu decyzyjnego, a każdy wiersz etykiety prognozowanej dotyczy wszystkich klas oddzielnie.

		Klasa rzeczywista		
		Pozytywna	Negatywna	
Klasa przewidywana	Pozytywna	Prawdziwie pozytywna (TP)	Fałszywie pozytywna (FP)	Czułość
	Negatywna	Fałszywie negatywna (FN)	Prawdziwie negatywna (TN)	Swoistość
Dokładność		Precyzja		

Rysunek 3.2: Graficzna prezentacja macierzy pomyłek dla problemu klasyfikacji binarnej.

Wprowadzając następujące oznaczenia dla danych predykcji:

- prawdziwie pozytywna (ang. *True Positives*, TP): poprawne dopasowanie przypadków pozytywnych,
- fałszywie pozytywna (ang. *False Positives*, FP): błędne dopasowanie przypadków negatywnych jako pozytywnych,
- fałszywie negatywna (ang. *False Negatives*, FN): błędne dopasowanie przypadków pozytywnych jako negatywnych,
- prawdziwie negatywna (ang. *True Negatives*, TN): poprawne dopasowanie przypadków negatywnych,

macierz pomyłek dla problemu klasyfikacji binarnej można przedstawić jak na rysunku 3.2. Dane zawarte w macierzy pomyłek otwierają możliwość wprowadzenia kolejnych miar oceny jakości klasyfikacji, takich jak:

- dokładność (ang. *Accuracy*) - to najpopularniejszy wskaźnik, który pozwala ocenić jaka część przypadków została zaklasyfikowana poprawnie:

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN}, \quad (3.33)$$

- precyzja (ang. *Precision*) - określająca, ile z przewidywanych pozytywnych przypad-

ków jest faktycznie pozytywnych:

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}}, \quad (3.34)$$

- czułość (ang. *Recall*) - wskazująca, jak dobrze klasyfikator określa rzeczywiste pozytywne przypadki:

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}}, \quad (3.35)$$

- swoistość (ang. *Specificity*) - jest miarą analogiczną do czułości, lecz dla przypadków negatywnych.

$$\text{Specificity} = \frac{\text{TN}}{\text{TN} + \text{FP}}, \quad (3.36)$$

- miara F1 (ang. *F1-score*) - średnia harmoniczna pomiędzy precyzją a czułością, łączącą oba wyznaczniki w jeden:

$$\text{F1-score} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}}, \quad (3.37)$$

Macierz pomyłek, mimo iż jest kluczowym narzędziem w procesie optymalizacji systemów opartych na uczeniu maszynowym, ma również swoje ograniczenia. W przypadku dużych, niebalansowanych zbiorów danych, gdzie widać wyraźną dominację jednej klasy nad drugą, znajdują zastosowanie dodatkowe kryteria.

3.6 Zakłócanie sygnałów radiowych

Walka radioelektroniczna jest stosunkowo młodą dziedziną sztuki wojennej, która zaczęła dynamicznie rozwijać się od początku XX wieku. Zasady z nią związane kształtowały się na przestrzeni lat i były różnie definiowane [89]. W aspekcie działań związanych z zakłócaniem sygnałów komunikacyjnych możemy spotkać w literaturze kilka metod kategoryzacji, a ta najbardziej klasyczna to podział z uwagi na formę generowanego sygnału [90]. Dodatkowo, sama strategia wykorzystania tych technik i związana z nią charakterystyka zachowania stacji zakłóceń stanowi osobny aspekt [91].

Podstawową ideą zakłócania jest doprowadzenie odpowiedniego sygnału do odbiornika urządzenia zakłócanego poprzez kanał radiowy. Gdy uda się zapobiec prawidłowemu funkcjonowaniu toru odbiorczego, proces ten uważany jest za skuteczny. Sytuacja ta może wystąpić, kiedy moc sygnału zakłócającego jest wystarczająco wysoka, lub jego kombinacja z sygnałem właściwym powoduje błędne dekodowanie danych. Miara efektywności danej stacji zakłóceń zazwyczaj wyrażana jest stosunkiem niezbędnej mocy fali zakłócającej J do fali właściwej S na wejściu odbiornika i określana skrótem J/S lub JSR (ang. *Jamming-to-Signal Ratio*). Korzystając z równania 3.12 dla modelu FSL oraz zakładając, że antena

odbiornika ma to samo wzmocnienie dla sygnału użytecznego i zakłócenia, zależność tę można zapisać jako 3.38:

$$JSR = \frac{\frac{P_j G_j G_r \lambda^2}{(4\pi d_j)^2}}{\frac{P_t G_t G_r \lambda^2}{(4\pi d_s)^2}} = \frac{P_j G_j d_s^2}{P_t G_t d_j^2}, \quad (3.38)$$

gdzie P_j oznacza moc sygnału zakłócającego, G_j wzmocnienie anteny źródła zakłócania, d_j odległość źródła zakłócania od anteny odbiorczej, d_s odległość nadajnika sygnału pożądanego od anteny odbiorczej, a pozostałe oznaczenia tożsame są z wzorem 3.12. Zapis w skali decybelowej można przedstawić w następujący sposób 3.39:

$$JSR_{dB} = P_j + G_j - P_t - G_t + 20 \log_{10} d_s - 20 \log_{10} d_j, \quad (3.39)$$

gdzie P_j i P_t wyrażone są w jednostkach dBW, G_j i G_t w dBi, a d_s i d_j w metrach [90]. Wartość JSR wymagana do przeprowadzenia skutecznego procesu zakłócania zależy od typu sygnału zakłócającego i modulacji transmisji. Stosunek JSR wynoszący 0 dB oznacza, że oba sygnały docierające do odbiornika są równe.

Wprowadzona wcześniej miara SNR, zależna od pasma odbiornika, jest istotna dla zagadnienia ogólnej analizy sygnałów. W systemach komunikacji satelitarnej natomiast, aby uniezależnić się od szerokości pasma i bezpośrednio wskazać jakość odbieranego sygnału, często używa się wskaźnika C/N_0 , który określa stosunek mocy nośnej do gęstości mocy szumu (ang. *carrier-to-noise-density ratio*). Zakładając, że układ wejściowy odbiornika jest jedynym źródłem zakłóceń, można przyjąć, że 3.40:

$$N_0 = kT, \quad (3.40)$$

gdzie k to stała Boltzmanna, a T jest temperaturą odbiornika. Wtedy, korzystając ponownie z równania 3.12, wskaźnik ten można zapisać jako 3.41:

$$C/N_0 = \frac{P_t G_t G_r}{kT} \left(\frac{\lambda}{4\pi d} \right)^2. \quad (3.41)$$

W skali decybelowej parametr C/N_0 wyrażany jest w jednostkach dB-Hz i można go sprowadzić do zapisu 3.42:

$$C/N_0 \text{ dB} = SNR + 10 \log_{10}(bw), \quad (3.42)$$

gdzie bw jest szerokością pasma odbiornika w hercach [92].

Kolejną miarą istotną z perspektywy zakłócania jest także E_b/N_0 , która przedstawia stosunek energii na bit do gęstości mocy szumu. Jest ona użyteczna przy porównywaniu bitowej stopy błędów transmisji (ang. *Bit Error Rate*, BER) w przekazie cyfrowym, przy

pominięciu wpływu szerokości pasma. W odniesieniu do C/N_0 można ją zapisać jako 3.43:

$$E_b/N_0 = C/N_0 \frac{1}{R_t}, \quad (3.43)$$

gdzie R_t oznacza przepływność bitową transmisji.

W ramach wstępu do teorii zakłócania warto także wspomnieć o twierdzeniu Shannona-Hartleya dotyczącym przepustowości kanału komunikacyjnego AWGN [80]. Wynika z niego, iż teoretycznie maksymalna przepustowość kanału C wyrażona w bitach na sekundę, ograniczona jest przez szerokość pasma B w hercach i stosunek sygnał-szum S/N w skali liniowej, zgodnie z zależnością 3.44:

$$C = B \log_2(1 + \frac{S}{N}). \quad (3.44)$$

Jeśli ilość informacji przesłana przez kanał jest mniejsza od jego pojemności, można zastosować specjalne techniki kodowania, które znacząco ograniczą stopę błędów w odbiorniku. W przeciwnym przypadku, na przykład na skutek wprowadzenia dodatkowego szumu, wzrost prawdopodobieństwa błędu będzie nieunikniony, niezależnie od sposobu kodowania.

3.6.1 Podstawowe techniki zakłócania

Zakłócanie zaporowe (ang. *barrage jamming*) bazuje na generowaniu przez stacje zakłóceń szumu losowego w celu zmniejszenia wartości SNR w zagłuszonym odbiorniku. Jest to technika, która nie wymaga żadnej wiedzy o strukturze sygnału właściwego, a proces zakłócania zazwyczaj przebiega w bardzo szerokim paśmie. Energia sygnału zakłócającego może być rozproszona na całe możliwe pasmo nadajnika, oddziaływać na dany kanał transmisji właściwej lub wpływać jedynie na wycinek widma.

Zakłócanie punktowe (ang. *tone jamming*) opiera się na generowaniu fali sinusoidalnej na jednej (ang. *single tone*) lub kilku (ang. *multiple tones*) strategicznie dobranych częstotliwościach. Pozwala to na większe skupienie energii niż w technice zaporowej, w celu skuteczniejszego wytrącenia zagłuszanego odbiornika z normalnych warunków pracy.

Zakłócanie przestrajane (ang. *sweep jamming*) podobne jest do zakłócania pojedynczym tonem, ale częstotliwość środkowa generowanego sygnału zmienia się w czasie. W tym przypadku fala zakłócająca może także przybrać formę szumu wąskopasmowego lub mieć cechy charakterystyczne zbliżone do sygnału właściwego. Prędkość przestrajania jest tutaj ważnym parametrem dla uzyskania odpowiednio szerokiego pokrycia widma, a zmiana częstotliwości środkowej odbywa się w sposób ciągły lub skokowy, dopasowany do sygnału zakłócanego.

Zakłócanie impulsowe (ang. *pulse jamming*) polega na wytwarzaniu krótkich impulsów o dużej mocy chwilowej, a ich generacja może przebiegać w systematycznych lub losowych

interwałach oraz z różnym wypełnieniem. Celem tej operacji jest oszukanie systemów radarowych lub wprowadzenie błędów bitowych w ramach komunikacyjnych, skutkujących ich odrzuceniem przez mechanizmy sprawdzania sum kontrolnych.

3.6.2 Wybrane strategie zakłócania

Nie istnieje jedna optymalna strategia zakłócania, a jej charakter zależy od warunków i obranej funkcji celu. Stosując taksonomię opartą na określeniu sposobu aktywacji nadajnika w stosunku do obiektu zakłócanego, niezależnie od samej zawartości transmisji, można wyróżnić podejście proaktywne i reaktywne [93].

Strategia proaktywna zakłada generowanie sygnałów niezależnie od obecności obiektu zakłócanego. Stacja z zakłócaniem ciągłym (ang. *constant jammer*) nastawiona jest na przełamanie mechanizmów wielodostępu do kanału radiowego, polegających na wykrywaniu nośnej przed rozpoczęciem transmisji przez urządzenie właściwe (ang. *Carrier-Sense Multiple Access*). Utrzymywanie pozorów ciągle zajętego kanału jest skuteczną i prostą w implementacji techniką, pochłania jednak dużo energii i jest łatwe do namierzenia. Bardziej zaawansowaną metodą, wymagającą większej wiedzy o strukturze zakłócanego sygnału, jest wstrzykiwanie w kanał pakietów, które zachowują pozory poprawnej transmisji, ale są wypełnione bezużytecznymi danymi (ang. *deceptive jammer*). Aby zoptymalizować kwestie poboru energii przez stacje, powstał także concept generowania zakłóceń przerywanych okresami uśpienia w sposób losowy lub adaptacyjny (ang. *random jammer*).

Strategia reaktywna zakłada monitorowanie widma oraz generowanie sygnałów zakłócających tylko w momencie obecności transmisji właściwej. Gdy stacja zakłóceń nie ma dokładnej wiedzy o protokole, reakcja wyzwalana przez detektor energii może odbywać się na zasadzie powtórzenia uprzednio nagranej, właściwej ramki komunikacyjnej, uzupełnionej o szum (ang. *repeater jammer*). Jeśli dokładna wiedza o docelowym protokole istnieje, nie tylko wykrycie transmisji w dostrojonym odbiorniku jest możliwe, ale także atak na warstwy wyższe niż fizyczna, jeśli istnieją tam znane podatności (ang. *protocol-aware jammer*). Mianem tym, szczególnie w kategorii związanej z zakłócaniem systemów nawigacji satelitarnej, określane też jest atak z dopasowaną do sygnału właściwego modulacją i prędkością bitową. O zakłócaniu inteligentnym mówimy natomiast, kiedy stacja jest w stanie zmieniać moc nadawania w sposób adaptacyjny, czy stosować metody oddziaływania tylko na fragmenty sygnału właściwego, odpowiadające za synchronizację czasu czy estymację kanału (ang. *smart jammer*).

Rozdział 4

Analiza bazy wiedzy w kontekście wybranej metody detekcji i przeciwdziałania bezzałogowym statkom powietrznym

4.1 Charakterystyka komercyjnych dronów

Bezzałogowe statki powietrzne można kategoryzować na kilka sposobów. Pierwszym z nich jest podział ze względu na fizyczną budowę urządzenia. Wyróżniamy tu konstrukcje jednowirnikowe, wielowirnikowe, skrzydłowe i hybrydowe. Drony wielowirnikowe stanowią najprostszą i najtańszą z wyżej wymienionych konstrukcji, dlatego zdominowały rynek komercyjny. Charakteryzują się one dodatkowo zdolnością zawisu i łatwością sterowania, co idealnie wpisuje się w potrzeby szeroko pojętego obrazowania powietrznego. Na dzisiaj najpopularniejszą formą są układy czterowirnikowe, choć liczba wirników coraz częściej jest zwiększana w celu poprawy udźwigu platformy.

W rozważaniach związanych z aplikacjami wojskowymi można stosować również podział ze względu na pułap operacyjny czy zasięg. Powyższe sposoby mogą być czasami utrudnione z uwagi na konstrukcje specjalne i układy hybrydowe. Wobec tego cywilna kategoryzacja Agencji Unii Europejskiej ds. Bezpieczeństwa Lotniczego bazuje na analizie ryzyka w potencjalnym zastosowaniu i opiera się na parametrze określającym masę startową obiektu [94]. Kategoria otwarta, charakteryzująca się niskim poziomem ryzyka przy założeniu braku złych intencji operatorów, określa graniczną masę startową drona na 25 kilogramów. Rysunek 4.1 przedstawia szczegółowy podział kategorii otwartej, w której zdobycie wymaganych uprawnień dla pilota komercyjnego statku bezzałogowego jest najmniej skomplikowane. Podział na podkategorie pod względem możliwości działania w bliskości skupisk ludzkich, czyli A1 i A2, zamyka się jednak w 4 kilogramach, co czyni

WHAT TYPE OF DRONE CAN I FLY?							
Operation			Drone Operator / pilot				
C-Class	Max Take off mass	Subcategory	Operational restrictions	Drone Operator registration?	Remote pilot qualifications	Remote pilot minimum age	
Privately build	<250g 	A1 Not over assemblies of people (can also fly in subcategory A3)	Operational restrictions on the drone's use apply (follow the QR code below)	Yes No if toy or not fitted with camera/sensor 	Read user's manual	No minimum age (certain conditions apply)	
legacy < 250g							
C0							
C1	<900g 				Yes	Check out the QR code below for the necessary qualifications to fly these drones	16
C2	<4kg 	A2 Fly close to people (can also fly in subcategory A3)					
C3	<25kg 	A3 Fly far from people					
C4							
Privately build							
Legacy drones (art 20)							



#EASAdrones

together
4safety

For more details go to
<https://www.easa.europa.eu/domains/civil-drones-rpas>



Rysunek 4.1: Podział na klasy dla komercyjnych dronów do 25 kilogramów w kategorii otwartej [94].

takie drony również najłatwiej dostępnymi w handlu.

4.1.1 Przegląd rynku

Pierwszy komercyjnie dostępny bezzałogowy statek powietrzny, który oferował wysoki poziom niezawodności oraz gotowość do lotu już w godzinę po wyjęciu z pudełka, został wprowadzony na rynek w 2013 roku przez firmę Shenzhen DJI Sciences and Technologies Ltd., znaną jako DJI. Platformę tę wyróżniał tryb precyzyjnego zawisu w momencie braku sterowania ze strony użytkownika, a zintegrowany w urządzeniu komputer pokładowy zapewniał łatwość obsługi nawet dla osoby z bardzo małym doświadczeniem. Do tej pory na rynku były dostępne tylko modele samolotów kontrolowanych zdalnie (ang. *Remote Contoled*, RC). Wymagają one wysokich umiejętności pilotażu, gdyż operator w tym przypadku posiada pełną kontrolę nad powierzchniami sterowymi. Proces zdobywania tych kwalifikacji jest skomplikowany, toteż modele RC pozostają jedynie w obrębie zainteresowań pasjonatów lotnictwa.

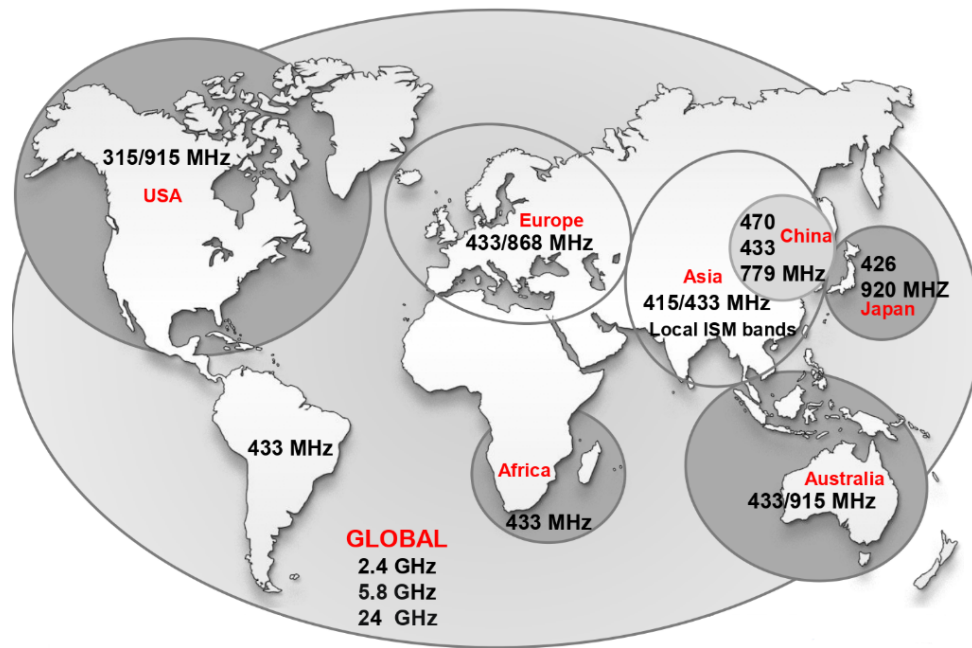
Pierwsza wersja najbardziej rozpoznawalnego drona firmy DJI nie posiadała zintegrowanej kamery. niespełna rok po premierze wprowadzono jednak model, który umożliwiał bezprzewodową transmisję obrazu. Do dziś z sukcesem rozwijanych jest kilka serii bezzałogowców w różnych klasach wagowych, a firma ta utrzymuje pozycję lidera pod względem wartości sprzedaży urządzeń komercyjnych. Popularność ta przyczyniła się do umieszczenia największej liczby modeli tej firmy w próbie doświadczalnej podczas dalszych eksperymentów związanych z detekcją i neutralizacją.

Firma DJI, jako pierwszy producent dronów komercyjnych o zasięgu globalnym, promowała również aspekty związane z bezpieczeństwem wykonywania lotów. Obecnie we wszystkich modelach o wadze powyżej 250 gramów montowane są specjalne odbiorniki, które informują operatora o bliskości innych systemów wyposażonych w transponder lotniczy [95]. Kiedy zagrożenie ze strony niewłaściwego użycia systemów dronowych zaczęło wzrastać, firma jako jedyna oferowała nawet dedykowany system lokalizowania platform powietrznych własnej produkcji. Określona grupa użytkowników mogła zakupić urządzenie, które dekodowało wysyłane radiowo dane o pozycji drona i operatora, na podstawie znajomości protokołów komunikacyjnych poszczególnych modeli [96]. Sprzedaż systemu została jednak wstrzymana w 2023 roku, co miało związek z wchodzącymi w życie regulacjami prawnymi dotyczącymi wspomnianych wcześniej nadajników identyfikacyjnych, jak komentuje producent. Kontrowersyjna może być decyzja ogłoszona w styczniu 2025 roku o dezaktywowaniu w oprogramowaniu przez producenta ograniczenia wynikającego z wirtualnych barier [97]. Do tej pory funkcja ta automatycznie blokowała możliwość operowania w przestrzeni lotnisk oraz infrastruktury krytycznej. Obecnie większa odpowiedzialność zostanie przeniesiona na użytkownika, a system zgłosi jedynie operatorowi komunikat o naruszeniu strefy.

4.1.2 Kanał sterowania i transmisji obrazu

Komunikacja bezprzewodowa pomiędzy komercyjnym statkiem bezzałogowym a operatorem opiera się na wykorzystaniu ogólnodostępnych częstotliwości radiowych ISM (ang. *Industrial, Scientific, and Medical*). Regulacje prawne dotyczące dostępnych pasm do nielicencjonowanej transmisji mogą różnić się między krajami, a ich rozkład geograficzny przedstawia rysunek 4.2. Globalny zasięg jednak pasm zwyczajowo określanych jako 2,4 GHz i 5,8 GHz uczynił je najczęściej wykorzystywanymi w systemach dronowych [98]. Pasma pierwsze obejmuje zakres częstotliwości od 2400,0 MHz do 2483,5 MHz i współdzielone jest z popularnymi systemami takimi jak Wi-Fi, Bluetooth czy ZigBee. Pasma drugie natomiast zawiera się w przedziale od 5725,0 MHz do 5875,0 MHz, gdzie operują sieci WiMAX (ang. *Worldwide Interoperability for Microwave Access*) czy WISP (ang. *Wireless Internet Service Provider*).

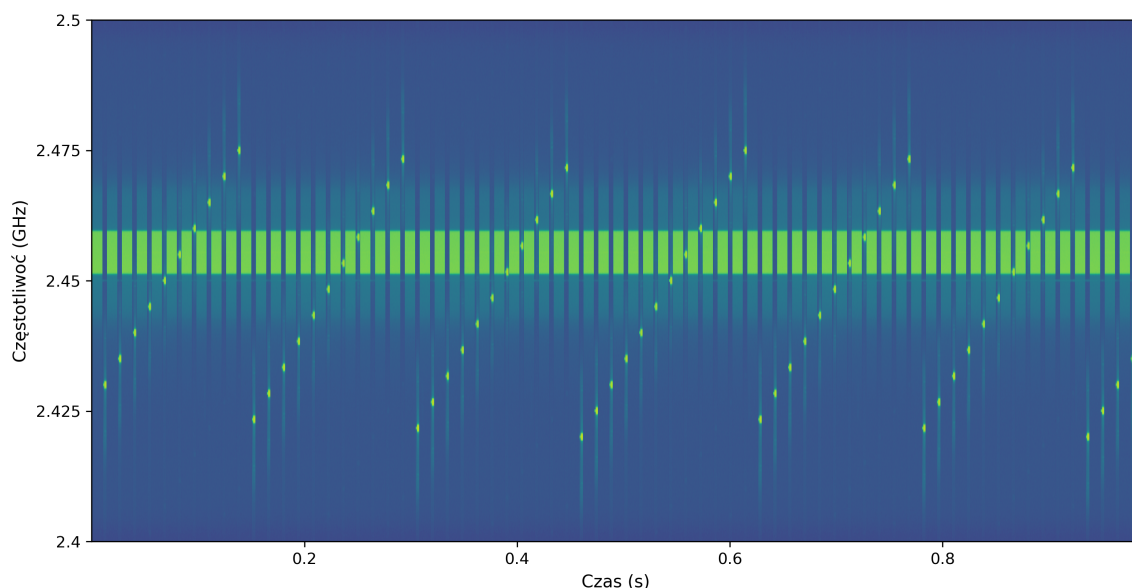
Kanał sterowania (ang. *uplink*), można zdefiniować jako transmisję danych od operatora do drona w celu przekazania niezbędnych komend do wykonywania czynności związanych z lotem czy obserwacją. W niektórych modelach możemy spotkać się ze skokową zmianą częstotliwości środkowej w każdej kolejnej ramce radiowej, co jest sposobem na zapewnienie operacji wielu urządzeń w tym samym paśmie. Jest to jedna ze znanych metod rozpraszania widma o nazwie FHSS (ang. *Frequency-Hopping Spread Spectrum*). Zmiany częstotliwości mogą mieć charakter pseudolosowy, jak w urządzeniach Bluetooth, lub sekwencyjny, jak na przykład w dronach firmy DJI [100].



Rysunek 4.2: Globalna alokacja pasm radiowych nie wymagających licencji [99].

Kanał zwrotny (ang. *downlink*) to transmisja od drona do operatora, w której zawarte są dane o statusie obiektu, takie jak położenie, prędkość czy wysokość, a także obraz z kamery na żywo. W tym przypadku nie występuje zmiana częstotliwości środkowej w każdej ramce, choć niektóre systemy są już w stanie czasem automatycznie wybrać kanał na podstawie analizy szumów w danym paśmie. Z uwagi na różne przeznaczenie obu kanałów, często charakteryzują się one innym sposobem modulacji czy szerokością pasma, a nawet mogą być rozdzielone pomiędzy poszczególne zakresy częstotliwości. Przykładowy obraz obu współistniejących w tym samym paśmie kanałów dla modelowego drona przedstawia w zapisie czasowo-częstotliwościowym rysunek 4.3.

Początkowo w systemach dronowych używano protokołu z rodziny 802.11, aby zrealizować zarówno sterowanie, jak i strumieniowanie wideo. Standard ten nie jest jednak przystosowany do takiego specyficznego zastosowania z uwagi na wymagane procesy wymiany potwierdzeń oraz narzut protokołu. Wprowadzało to ograniczenia w zasięgu oraz wpływało na opóźnienie obrazu transmitowanego na żywo. Powyższe wady skłoniły producentów do opracowania autorskich protokołów wymiany danych, z których każdy jest dostosowany do indywidualnego rozwiązania, głównie w kategorii kosztu i rozmiaru urządzenia. Dokładna specyfikacja protokołów stanowi tajemnicę przedsiębiorstw, ale badacze przeprowadzili pewne analizy, dzięki którym możemy powiedzieć więcej o tych rozwiązaniach. Pierwszym z nich jest Enhanced Wi-Fi, stworzony na potrzeby niewielkich modeli, którego zastosowanie pozwala wydłużyć zasięg transmisji z 500 m do 2000 m, wciąż przy niewielkim koszcie. Kolejnym systemem jest Lightbridge, który oferuje łączność na odległość do 3600 m oraz znacznie mniejsze opóźnienie obrazu. Protokół OcuSync natomiast, pozostając w zgodzie z limitami emisji mocy, pozwala na podwojenie tego zasięgu oraz



Rysunek 4.3: Zapis czasowo-częstotliwościowy izolowanego sygnału dronowego. Kanał transmisji szerokopasmowej posiada stałą częstotliwość środkową, podczas gdy kanał sterowania wykonuje okresowe przeskoki.

automatyczne przełączanie się pomiędzy pasmami ISM 2,4 GHz i 5,8 GHz [101].

Wymienione powyżej protokoły i ich autorskie modyfikacje bazują na technice polegającej na jednoczesnej transmisji wielu strumieni danych na ortogonalnych podnośnych (ang. *Orthogonal Frequency-Division Multiplexing*, OFDM). Koncepcja ta polega na zastąpieniu jednej szybkiej transmisji przez kilka wolnych strumieni i jest sposobem na uniknięcie problemów związanych z wielodrogowością. Liczba podnośnych niosących dane, jak i liczba kanałów pilotowych służących do estymacji zjawisk w kanale radiowym mogą być dostosowane do konkretnego scenariusza. Najczęściej stosowanymi modulacjami w podnośnych są modulacje fazowe (ang. *Phase Shift Keying*, PSK) oraz amplitudowo-fazowe (ang. *Quadrature Amplitude Modulation*, QAM). Ten tryb transmisji wymaga złożonej architektury zarówno nadajnika, jak i odbiornika, a dane dodatkowo uzupełniane są o kody korekcyjne w celu zwiększenia niezawodności łącza bezprzewodowego. Ilość danych przesyłanych przez kanał w przypadku bezzałogowych statków powietrznych jest zazwyczaj większa w odniesieniu do modeli RC, gdzie stosowane są zazwyczaj modulacje z kluczowaniem częstotliwości (ang. *Frequency-Shift Keying*, FSK). W niektórych opracowaniach urządzenia te nie są rozróżniane, jednak ta praca skupia się głównie na dronach, z uwagi na łatwiejszy dostęp do nich oraz szerszą możliwość niebezpiecznego użycia.

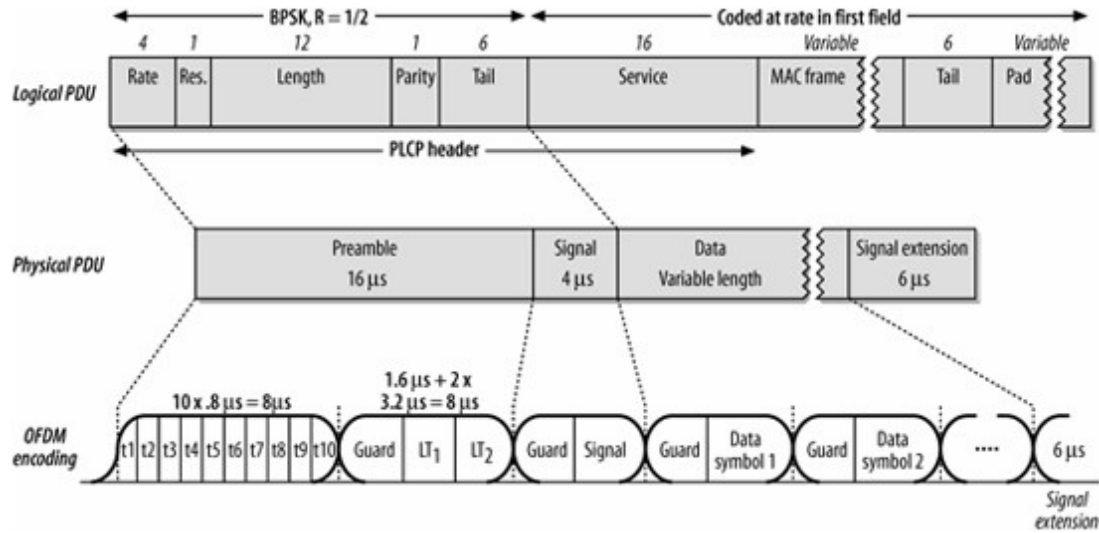
Standardy z rodziny 802.11 różnią się między sobą, podobnie jak protokoły stosowane przez producentów bezzałogowych statków powietrznych. Istnieją jednak pewne ogólne wytyczne dotyczące budowania warstwy fizycznej ramki radiowej opartej na OFDM. Przedstawione zostaną na przykładzie standardu 802.11g o paśmie 20 MHz, który pojawia się również w analizie literaturowej jako pewien punkt odniesienia. Format ten składa się

sumarycznie z 52 ortogonalnych podnośnych, z których 4 zarezerwowane są na piloty, a pozostałe modulowane są symbolami danych. Każda ramka radiowa rozpoczyna się preambułą zbudowaną z 12 symboli i jest podzielona na dwie sekcje po 8 μs . Pierwszy element zawiera 10 krótkich symboli, transmitowanych wyjątkowo na 12 podnośnych, i służy do wykrywania startu transmisji, ustawiania regulacji wzmocnienia oraz zgrubnej korekcji częstotliwości nośnej. Element drugi zawiera dwa długie symbole transmitowane na 52 podnośnych i pomaga w estymacji kanału oraz dokładnej korekcji częstotliwości. Po preambule umieszczony jest jeden symbol nagłówka, w którym zawarte są informacje o typie modulacji, a po nim następuje transmisja danych. Podstawowa długość symbolu w części zawierającej dane wynosi 4 μs , a poszczególne podnośne są rozmieszczone co 312,5 kHz. W skład symbolu wchodzi także prefiks cykliczny, który jest skopiowanym na początek każdego symbolu jego końcowym fragmentem. Operacja ta ma na celu poprawę aspektów związanych z wielodrogowością. Długość zastosowanych prefiksów cyklicznych jest stała i wynosi 0,8 μs , czas trwania całej ramki w tym standardzie jednak może być zmienny. Transmisję zamyka pojedyncza sekcja trwająca 6 μs , pomagająca spełnić zależności czasowe [102]. Budowa tej ramki przedstawiona jest symbolicznie na rysunku 4.4a, a jej reprezentacja w dziedzinie czasu pokazana jest na rysunku 4.4b.

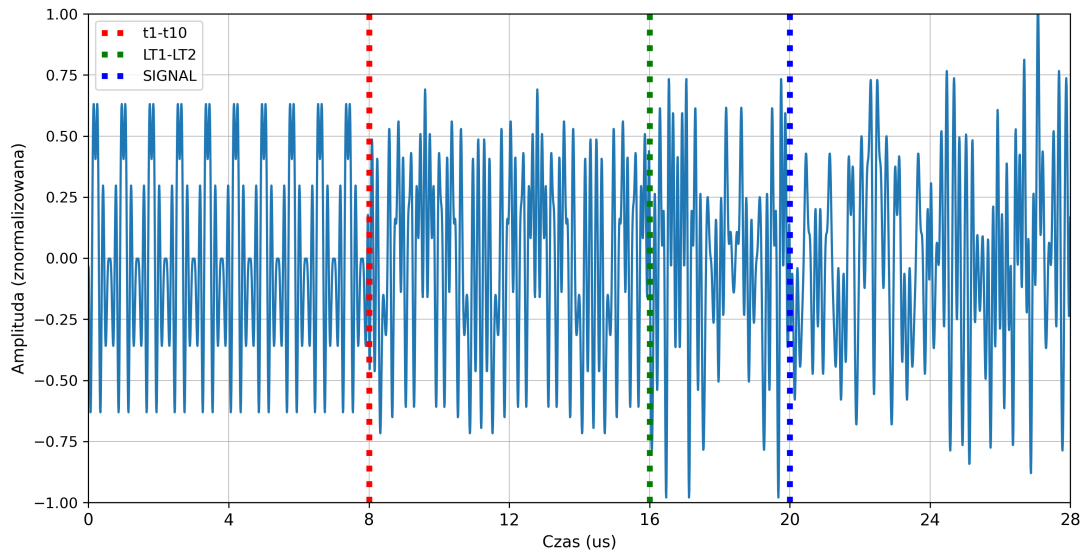
4.1.3 Odbiornik nawigacji satelitarnej

Bezzałogowe statki powietrzne do ustalania lokalizacji w przestrzeni oraz pomiaru prędkości względem ziemi używają systemu nawigacji satelitarnej. Dzięki temu mogą wykonywać loty po zadanej trasie lub autonomicznie wracać do miejsca startu na polecenie operatora. Sygnały te są również wykorzystywane do kompensacji dryfu czujników inercyjnych podczas utrzymywania pozycji w zawisie. Utrata sygnału nawigacyjnego jest komunikowana operatorowi jako pewnego rodzaju sytuacja awaryjna. Odbiorników nawigacyjnych zazwyczaj nie posiadają drony wyścigowe oraz zabawkowe, przeznaczone do operacji w pomieszczeniach zamkniętych.

Globalnie, dla komercyjnego użytku, dostępne są cztery niezależne systemy nawigacji satelitarnej (ang. *Global Navigation Satellite System*, GNSS): GPS, Galileo, GLONASS i BeiDou. Nowoczesne moduły odbiorcze potrafią obliczać pozycję, wykorzystując dane z kilku systemów jednocześnie, a dzięki zastosowaniu rozpraszania kodowego (ang. *Direct Sequence Spread Spectrum*, DSSS), poziom sygnału w odbiorniku może być mniejszy od szumu. Podstawą działania tej techniki jest mnożenie strumienia danych przez indywidualny dla każdego satelity ciąg kodowy, a najczęściej występującą modulacją jest binarne kluczowanie fazy (ang. *Binary Phase Shift Keying*, BPSK). Wyjątkiem jest system GLONASS, który stosuje ten sam kod dla wszystkich satelitów, gdzie każdy z nich nadaje na innej częstotliwości.



(a) struktura blokowa [102]



(b) zapis czasowy

Rysunek 4.4: Reprezentacja budowy ramki protokołu 802.11g, z zaznaczonymi podziałami na elementy składowe.

Na przykładzie budowy urządzeń GPS można podzielić typ kodowania na zgrubne (ang. *Coarse Acquisition*, C/A) oraz precyzyjne (ang. *Precision*, P). Kod P jest używany w zastosowaniach wojskowych i posiada dodatkowe zabezpieczenia w postaci szyfrowania, które chroni przed intencjonalnym oszukiwaniem wskazań pozycji. Kod C/A natomiast to sekwencja o długości 1023 bitów PRN (ang. *Pseudorandom Noise*), która powtarza się z okresem jednej milisekundy. Zastosowanie ortogonalnych sekwencji kodowych pozwala na nadawanie przez satelity sygnałów na tych samych częstotliwościach, a docierają one do ziemi z mocą od -125 dBm do -150 dBm. Synchronizacja poszczególnych kodów przebiega równolegle w wielu kanałach odbiornika, a jeśli jest ona utrzymana dla odpowiedniej liczby satelitów, to wyznaczenie różnic w czasie przelotu sygnału z orbity do odbiornika pozwala

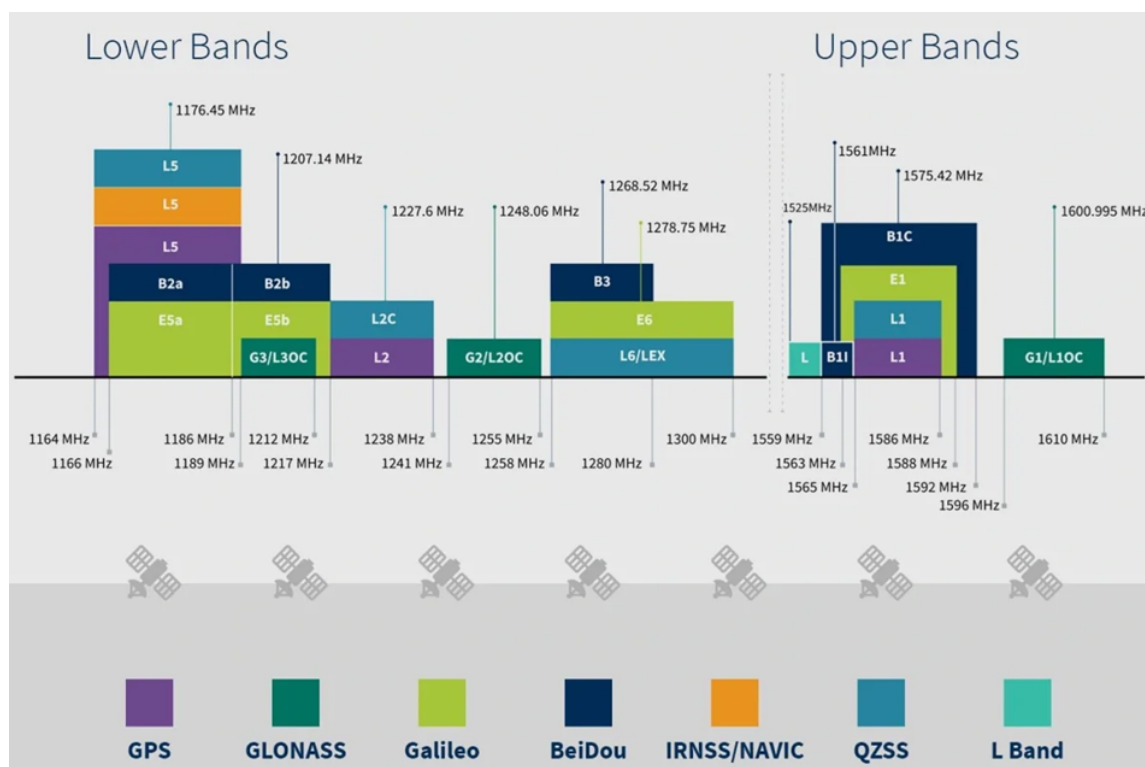
na określenie położenia.

Aby wyznaczyć pozycję, odbiornik potrzebuje jeszcze dodatkowych informacji o sieci satelitów. W tym celu na kod C/A nałożona jest depesza nawigacyjna, nadawana z prędkością 50 bps, składająca się z 1500 bitów i podzielona na pięć ramek. Jej transmisja zajmuje 6 s. Ramka pierwsza informuje o statusie satelity oraz zawiera datę i czas. Ramka druga i trzecia zawierają efemerydy konieczne do obliczenia pozycji satelitów w momencie obserwacji. W czwartej i piątej ramce zapisane są części almanachu zawierające dane o wszystkich satelitach w konstelacji. Aby odebrać całość almanachu, potrzebne jest 25 depesz oraz czas wynoszący 12,5 minuty. Dane o efemerydach są ważne nie dłużej niż 4 godziny i mogą być pobrane zaraz po włączeniu zasilania odbiornika, podczas gdy almanach, zawierający bardziej ogólne informacje, obowiązuje przez 180 dni i pomaga w określeniu, jakich satelitów należy poszukiwać.

Podstawowe częstotliwości nośne dla GPS to L1: 1575,42 MHz ($10,23 \text{ MHz} \times 154$), L2: 1227,60 MHz ($10,23 \text{ MHz} \times 120$) oraz L5: 1176,45 MHz ($10,23 \text{ MHz} \times 120$). Mapa podziału częstotliwości między wszystkimi konstelacjami przedstawiona jest na rysunku 4.5. Pojawiają się tu także systemy, niewspomniane wcześniej, takie jak QZSS oraz NAVIC, oferujące jedynie zasięg lokalny odpowiednio w rejonie Japonii oraz Indii, a także pasmo przeznaczone na sygnały korekcyjne, oznaczone jako L-BAND. Producenci komercyjnych dronów zazwyczaj podają, z jakich systemów nawigacyjnych korzysta urządzenie, nie zawsze jednak specyfikują konkretne zakresy częstotliwości. Jednakże analizy wskazują, że powszechnie jest to pasmo L1 [98], które opiera się na dojrzałej technologii. Odbiorniki wielozakresowe, wykorzystujące pasma L1/L2 lub L1/L5, oferują wprowadzić lepszą dokładność, jednakże wymagają zwiększonego poboru prądu oraz bardziej skomplikowanego układu antenowego, co powoduje ich mniejszą popularność w zastosowaniach konsumenckich. Z uwagi na zakres rozprawy, obejmujący komercyjnie dostępne urządzenia, w aspekcie sygnałów GNSS skupiono się także na sygnałach cywilnych.

4.1.4 Nadajnik zdalnej identyfikacji

Odkąd problem związany z niebezpiecznym użyciem dronów stał się tematem globalnym, rozpoczęto dążenie do wprowadzenia zunifikowanej metody monitorowania ruchu komercyjnych statków bezzałogowych. Prekursorem tych działań była administracja w Stanach Zjednoczonych, a inne kraje podążały za nią, wprowadzając drobne modyfikacje. Istotą systemu RemoteID jest integracja na dronie nadajnika radiowego, który rozgłasza unikalne dane identyfikacyjne drona, jego pozycję oraz lokalizację operatora. Zestaw danych nieznacznie różni się w zależności od organu regulacyjnego. Zasady te w pełni obowiązują w Stanach Zjednoczonych od 2023 roku, a Unia Europejska wprowadziła je prawie rok później [104].



Rysunek 4.5: Podział pasm częstotliwości pomiędzy poszczególne systemy nawigacji satelitarnej [103].

Od obowiązku instalacji nadajnika istnieją jednak pewne wyjątki, które wciąż pozostawiają przestrzeń na działania niepożądane. Wyłączenie dotyczy na przykład maszyn o masie poniżej 250 gramów, co jest poparte badaniami ryzyka utraty zdrowia człowieka związanego z energią uderzenia takiego obiektu [43]. Sytuacja niebezpieczna jednak, w której dron o tej masie zderzył się z samolotem do walki z pożarami, miała miejsce w styczniu 2025 roku [105]. Mimo uszkodzenia poszycia skrzydła, wprawdzie nie doszło bezpośrednio do katastrofy lotniczej, ale płatowiec wyłączony był z akcji gaśniczej na kilka dni. Jak wskazują badania, kolizje te są groźne także dla samolotów pasażerskich, gdyż, mimo niewielkich uszkodzeń mechanicznych, może dojść do przecięcia wiązek kablowych i w konsekwencji utraty sterowności [106].

Na terenie Stanów Zjednoczonych wydzielone są także specjalne strefy rekreacyjne, w których wymaganie instalacji nadajnika nie obowiązuje. W Unii Europejskiej natomiast producenci zobligowani są do montażu identyfikatora dopiero od stycznia 2024 roku. Wprawdzie zadeklarowano w stosunku do kilku starszych modeli możliwość aktualizacji oprogramowania, w innych natomiast przypadkach użytkownik sam będzie musiał wyposażyć się w nadajnik zewnętrzny. Pokazuje to, że wciąż w wykorzystaniu znajduje się ogromna liczba urządzeń nieposiadających tego systemu. Dodatkowo pojawiają się, niestety, wpisy na forach internetowych z poradami, jak wyłączyć lub oszukać nadajniki zdalnej identyfikacji. Jednym ze znanych sposobów jest celowe oszukiwanie odbiorników nawigacji satelitarnej i zakłamanie rozgłaszanej pozycji [107].

Uniwersalność rozwiązania proponowanego dla powszechnego monitorowania pozycji systemów bezzałogowych wymagała zastosowania w nadajniku najpopularniejszych protokołów bezprzewodowych używanych w dzisiejszych komputerach przenośnych oraz smartfonach. Tym samym regulacje wskazują na możliwość wykorzystania standardów Wi-Fi lub Bluetooth, głównie w zakresie otwartego pasma 2,4 GHz, z maksymalną dozwoloną mocą promieniowania. Dla standardu Wi-Fi wytypowano kanał 6, czyli zakres częstotliwości 2426-2448 MHz, choć alternatywnie, na przykład w Japonii, można używać także kanału 149 o zakresie 5735-5755 MHz. Dla standardu Bluetooth natomiast są to kanały 37, 38 i 39, zajmujące odpowiednio częstotliwości środkowe 2402 MHz, 2426 MHz oraz 2480 MHz. Podejście to pozwala na wykrycie dronów operujących w pobliżu poprzez aplikację na telefonie lub konstrukcję urządzenia opartego na komputerze jednopłytkowym wraz z kartą radiową [101].

Choć inicjatywa unifikacji systemu monitorowania ruchu dronowego wydaje się słuszna, zyskała ona także pewne grono przeciwników. Głównym argumentem może być tutaj prywatność operatora oraz możliwość dostępu osób postronnych do planowanej trasy przelotu statków bezzałogowych dostarczających paczki [108]. Badania nad systemami alternatywnymi wciąż trwają, zaproponowano też szereg ulepszeń związanych z szyfrowaniem wysyłanych wiadomości oraz dalszym rozwojem protokołów komunikacyjnych [109].

4.2 Przegląd prac z zakresu wykrywania BSP

Proces wykrywania obecności statków bezzałogowych metodą radiową obejmuje przechwytywanie sygnałów komunikacyjnych, ekstrakcję cech i ich identyfikację. Następnie wyróżniamy etap detekcji, w którym podejmowana jest binarna decyzja o obecności drona, a w dalszej kolejności możemy przystąpić do klasyfikacji konkretnego modelu. Oba kroki mogą też zostać scalone w jeden proces, na przykład przy użyciu metod uczenia maszynowego. W niniejszej pracy skupiono się przede wszystkim na wykryciu zagrożenia, gdyż różnorodność modeli na rynku jest obecnie ogromna. Dodatkowo, producenci ze względów ekonomicznych często stosują te same komponenty w różnych produktach, co komplikuje proces dokładnej klasyfikacji, wydłuża obliczenia, a nawet okres akwizycji danych. Dokonując przeglądu różnych sposobów detekcji, wspomniano o kategoryzacji technik radiowych, która rozróżnia urządzenia zastosowane do pozyskiwania sygnału. Szczegółowa synteza prac badawczych przeprowadzona będzie z wyróżnieniem dziedziny, w której poszczególne cechy będą poddawane analizie.

4.2.1 Protokół radiowy

Pierwszą kategorię stanowią sposoby oparte na znajomości protokołu radiowego zastosowanego w połączeniu bezprzewodowym pomiędzy dronem a operatorem. Istnieje wciąż

pewna grupa dronów działająca przy użyciu standardowego protokołu Wi-Fi, a więc do analizy sygnału można również użyć łatwo dostępnych urządzeń przechwytyjących pakiety. Część dronów operujących w tej kategorii posiada charakterystyczny numer MAC (ang. *Media Access Control*) lub nazwę sieci Wi-Fi, które mogą służyć do ich identyfikacji [110]. Na podstawie modelowania procesu dolotu drona do chronionego obiektu stacjonarnego, wykonać można także badanie zmienności RSSI (ang. *Received Signal Strength Indication*), wskazujące na potencjalną obecność intruza [111]. W podejściu opartym na podobnej metodzie dodatkowo rozdzielono proces decyzyjny na model SVM, gdy istnieje bezpośrednia widoczność nadajnika i odbiornika, oraz LSTM w przypadku przeciwnym [112].

Wnioskowanie na podstawie zagęszczenia ruchu sieciowego w monitorowanej przestrzeni jest również przedmiotem badań [31]. W przypadku zaszyfrowanych sieci Wi-Fi analiza parametrów, takich jak wielkość pakietów oraz czas pomiędzy ich wysłaniem, pozwala nawet na klasyfikację trybu pracy poszczególnych modeli [113]. Wchodząc jeszcze głębiej w przestrzeń danych przesyłanych drogą radiową, udało się rozszyfrować jeden z autorskich protokołów, uzyskując dokładne informacje o pozycji drona [114]. Powyższe techniki, mające na celu wykrycie statków bezzałogowych emitujących intencjonalnie sygnały oparte na znanych standardach bezprzewodowych, zostały zintegrowane w pracy [101]. Detektor powstał na podstawie komercyjnie dostępnych produktów i składał się głównie z komputera jednopłytkowego (ang. *Single Board Computer*, SBC) oraz dwóch kart sieciowych do równoległej analizy w kilku pasmach radiowych. W odróżnieniu od powyższej metody, w kolejnych kategoriach wymagany jest dostęp do zapisu sygnału radiowego, skwantowanego do postaci cyfrowej.

4.2.2 Dziedzina czasu

Analiza w dziedzinie czasu może odbywać się już na surowych próbkach sygnału radiowego. Z jednej strony pozwala to na badanie krótkiego fragmentu danych, z drugiej jednak mogą zostać pominięte cechy charakterystyczne związane z czasem trwania ramki oraz odstępem między transmisjami. Interesującym aspektem tej metody jest natomiast możliwość rozróżnienia tych samych modeli dronów pozostających w zawisie na podstawie subtelnych niedoskonałości analogowego toru nadawczego [115]. Osiągnięcie dokładności detekcji na poziomie 99,41% jest wprawdzie możliwe dzięki zastosowaniu sieci CNN, aczkolwiek sygnał poddany interpretacji musi być wolny od zakłóceń [116]. Bezpośrednie porównanie natomiast pomiędzy sieciami DNN i CNN dało w przypadku problemu decyzji binarnej o obecności drona wyniki odpowiednio 99,50% i 99,70% [117]. Przy tej samej bazie danych, proponując autorską architekturę samej sieci i prowadząc jednocześnie optymalizację w aspekcie złożoności obliczeniowej, udało się polepszyć ten wynik do 99,85% [118].

Przeprowadzając badania poza izolowanym środowiskiem, należy dodatkowo uwzględnić obecność innych sygnałów radiowych pozostających w paśmie odbiornika podczas pozyskiwania danych. Zastosowanie podejścia dwustopniowego, czyli wstępne oddzielenie transmisji Wi-Fi i Bluetooth od sygnałów dronowych, jest wykonalne w dziedzinie czasu tylko wtedy, gdy sygnały te nie występują jednocześnie. W odróżnieniu od powyższych metod, w których analizowany był surowy sygnał bez wstępnego przetwarzania, do stworzenia zestawu cech można także wykorzystać skok energii, oznaczający początek transmisji radiowej [33]. W pierwszym kroku jednak należy oddzielić sygnał od szumu, co udało się osiągnąć przy pomocy naiwnego klasyfikatora Bayesa, osiągając dokładność na poziomie 96,6% przy 2 dB SNR. Następnie zbudowanie zestawu kilkunastu parametrów statystycznych, takich jak współczynnik skośności czy kurtoza, oraz finalne zastosowanie szeregu metod uczenia maszynowego pozwoliło na osiągnięcie dokładności klasyfikacji na poziomie 98,13% przy stosowaniu algorytmu KNN w warunkach 25 dB SNR.

Wrażliwość tej metody na zmienność stosunku sygnału do szumu może zostać zminimalizowana poprzez zastosowanie w zbiorze treningowym danych o większym zróżnicowaniu. Wyjściowa dokładność na poziomie 97,53% osiągalna jest wtedy w całym zakresie SNR od 0 dB do 30 dB [119]. Poza cechami statystycznymi, w procesie decyzyjnym można użyć parametrów ściśle związanych z typem modulacji, co stanowi szczególny przypadek analizy w dziedzinie czasu. Zakładając, że większość protokołów transmisji obrazu oparta jest na technice OFDM, ekstrakcja cech, takich jak długość symbolu oraz czas trwania prefiksu cyklicznego, pozwala na osiągnięcie dużo lepszych rezultatów w porównaniu do metod statystycznych [120].

4.2.3 Dziedzina częstotliwości

Analiza widmowa wymaga przekształcenia cyfrowego sygnału z dziedziny czasu do dziedziny częstotliwości za pomocą operacji matematycznych. Pozwala to na ujawnienie dodatkowych cech w zbiorze przetwarzanych danych, a także na wstępne rozdzielenie sygnałów właściwych od zakłóceń, jeśli nie zajmują one tego samego pasma. Wykorzystując w ten sposób blok danych o długości 250 ms oraz metodę DNN, osiągnięto nawet dokładność detekcji na poziomie 99,7%, jednak przy zachowaniu wysokiego SNR [121]. Bazę treningową dla rozwiązania problemu binarnego stanowiły w tym przypadku zgrupowane sygnały dronowe oraz aktywności tła. W eksperymencie zaproponowano także dodatkową sieć, w której ten sam zbiór sygnałów statków bezzałogowych rozdzielono na trzy typy, uzyskując rozwiązanie zadania klasyfikacji grupy czteroelementowej z dokładnością równą 46,8%. Wprowadzając podejście hierarchiczne przy tej samej bazie danych, można również przeprowadzić najpierw detekcję, a dopiero w przypadku obecności obiektu klasyfikację w grupie trzejelementowej, co zwiększa dokładność do 99,2% przy użyciu techniki KNN [122].

Interesującym podejściem jest także rozdzielenie detekcji i klasyfikacji, nie tylko w podejściu hierarchicznym, ale także w architekturze zastosowanej sieci. Podział tych zadań pomiędzy DNN i CNN odpowiednio dał najlepsze rezultaty w tej kategorii [123]. Operując w dziedzinie częstotliwości, możliwe jest również zastosowanie parametrów statystycznych jako cech wejściowych dla metod uczenia maszynowego. Korzystając z zestawu trzech takich wyznaczników, przy wysokim SNR można uzyskać dokładność równą 96,36% [124]. Zwracając uwagę dodatkowo jednak na aspekt odległości obiektu od układu pomiarowego, wartość ta spada do 84,77% przy dystansie dwóch kilometrów. W badaniu zaproponowano trzywarstwową architekturę ANN oraz wykazano jej przewagę nad metodami SVM i KNN. Rozszerzenie zbioru parametrów statystycznych do trzydziestu, przy wykorzystaniu cech z obu dziedzin, dało finalny efekt zwiększenia dokładności do 95,52% przy tej samej odległości [125]. Podczas eksperymentów porównano również metody ANN i SVM, ale w tym przypadku najlepszy okazał się klasyfikator oparty na podejściu RDF.

4.2.4 Spektrogram

Analiza w dziedzinie czasu oraz częstotliwości może być stosowana indywidualnie lub przy wykorzystaniu fuzji danych pozyskanych równoległe z dwóch form reprezentacji sygnału. Spektrogram, czyli wykres widma amplitudowego przedstawiony w czasie, łączy zalety obu metod w jednej formie zapisu. Odpowiednio dobrana długość FFT pozwala na ekstrakcję cech takich jak długość trwania ramki radiowej, odstęp między kolejnymi sygnałami czy wartość przeskoku częstotliwości w technice FHSS [34]. Traktując spektrogramy jako obrazy dwuwymiarowe, można je wykorzystać nawet bezpośrednio w zbiorze treningowym do detekcji dronów przy pomocy różnych technik uczenia maszynowego. W jednym z eksperymentów, przy zestawieniu tych metod, najlepsze rezultaty w całym zakresie pomiarowym zostały osiągnięte przy użyciu RNN, a w przypadku wysokiego SNR tylko mechanizm SVM osiągnął podobny rezultat [126]. Zastosowanie metody opartej na spektrogramie pozwala teoretycznie zwiększyć przede wszystkim dokładność klasyfikacji nawet do 99,99%, przy zamkniętym zbiorze czteroelementowym i wysokim SNR [127]. Zestawienie pokazało podobne wyniki dla technik ANN i KNN, a najgorzej wypadło podejście oparte na DT.

W praktyce jednak kanały radiowe, na których operują komercyjne statki bezzałogowe, są dodatkowo dynamicznie zmieniane, co znacznie komplikuje to zagadnienie. Jednym ze sposobów rozwiązania tego problemu jest wstępna korekcja przesunięcia częstotliwości środkowej sygnału użytecznego [128]. W przytoczonym artykule autorom udało się porównać dwa podejścia, działając na tym samym zbiorze treningowym i korzystając z wariantów CNN. Przy braku korekcji określono wprawdzie skuteczność metody opartej na spektrogramie na poziomie 99,72%, ale tylko podczas obecności sygnału drona na kanale znajdującym się w zbiorze treningowym. W przeciwnym przypadku notowano spadki wyniku nawet do

16,97%. Po wprowadzeniu kompensacji przesunięcia częstotliwości dokładność nie spadała jednak poniżej 98%, niezależnie od kanału. Finalnie wykazano, że ogólna skuteczność tego podejścia wynosi 99,29%, podczas gdy niezależne analizy w dziedzinie czasu czy częstotliwości dały odpowiednio 83,10% i 88,48% przy tej samej bazie treningowej.

Powyższe eksperymenty wskazały wprawdzie na skuteczność metod opartych na spektrogramie i sieciach neuronowych, jednakże nie brano w nich pod uwagę zagadnienia zmienności SNR. Rozpatrując ten aspekt, w pierwszej kolejności można przywołać eksperyment wskazujący, że w warunkach malejącego SNR analiza sygnału w dziedzinie czasu sprawdza się gorzej niż podejście bazujące na spektrogramie [129]. Generacja tej formy zapisu to zawsze również kompromis pomiędzy rozdzielczością czasową a częstotliwościową. W warunkach niskiego SNR redukcja rozdzielczości częstotliwościowej ma mniejszy wpływ na skuteczność sieci neuronowych niż spadek rozdzielczości czasowej zapisu. Zastosowanie tego priorytetu zwiększyło dokładność metody opartej na CNN z 32% do 60% dla sygnałów o SNR równym -10 dB [130].

Poza wpływem SNR na skuteczność detekcji istotny jest także temat odniesienia badań laboratoryjnych do realnego środowiska elektromagnetycznego. Prawdopodobieństwo detekcji sieci neuronowej trenowanej na zbiorze izolowanych danych pochodzących z komory bezodbiciowej, odniesione do warunków rzeczywistych, spada nawet przy dobrej jakości sygnału do 75% [131]. Dalsze eksperymenty, przeprowadzone również na podstawie analizy czasowo-częstotliwościowej, wykazały, że ta sama sieć trenowana na danych rzeczywistych zapewnia skuteczność na poziomie 93%. Główną ideą przytaczanej pracy było wykazanie, że istotne jest zawieranie w bazie danych uczących zarówno sygnałów rzeczywistych, jak i tych pozyskanych poprzez modelowanie w środowiskach wirtualnych. Podejście to pozwoliło na podniesienie wyniku detekcji do 97%. Aspekt poboczny, ale także ważny dla praktycznego zastosowania, stanowiła optymalizacja architektury samej sieci wykorzystanej w badaniach porównawczych. Jako referencje wykorzystano standardową sieć YOLOv5s, która zarówno w zadaniu detekcji, jak i klasyfikacji przy SNR -10 dB dała wyniki tylko o około 2% lepsze, przy siedmiokrotnie większej złożoności.

Podejście oparte na CNN, trenowane na pozyskanych w przestrzeni laboratoryjnej spektrogramach, uzupełnionych o sztucznie wygenerowany szum, posiada wysokie zdolności do generalizacji, nawet w środowisku rzeczywistym [132]. W prezentowanych badaniach porównano różne architektury sieci głębokich, od VGG11 do VGG19 (ang. *Visual Geometry Group*), zarówno w zadaniu detekcji, jak i klasyfikacji [133]. Dla SNR powyżej -4 dB wszystkie sieci wykazały nasycenie dokładności, a znaczący spadek zaobserwowano dopiero poniżej -12 dB. Różnice między nimi nie były istotne, więc do dalszych testów wybrano najprostszą topologię. W środowisku rzeczywistym pomiary dokładności detekcji na odległości 110 m wyniosły 95,5%, a na 670 metrach 92,5%. W zadaniu klasyfikacji sześćoelementowej natomiast, gdzie jedną z klas stanowił szum, zanotowano wyniki odpowiednio 85,2% i 70,8%. Szczegółowa obserwacja macierzy pomyłek wskazała, że w prezentowanej meto-

dzie znacznie częściej dochodzi do błędów klasyfikacji pomiędzy sygnałami dronowymi a szumem niż w zadaniu rozróżnienia między konkretnymi modelami urządzeń.

4.3 Przegląd prac z zakresu przeciwdziałania BSP

Baza opracowań w temacie przeciwdziałania bezzałogowym statkom powietrznym drogą emisji fal radiowych jest znacznie bardziej okrojona niż w aspekcie detekcji. Spowodowane to jest nie tylko aspektami etycznymi, ale także ograniczeniami prawnymi. Przeprowadzanie testów w warunkach laboratoryjnych jest wprawdzie możliwe w niektórych przypadkach, jednak czasami trudno jest odnosić je do rzeczywistego środowiska. Dodatkowo, stosowane przez producentów autorskie protokoły wymiany danych nie pozwalają na dokładną ocenę jakościową skuteczności zakłócania ani na modelowanie zachowań odbiornika w środowisku wirtualnym.

W aspekcie detekcji porównania między różnymi algorytmami, w odniesieniu do dziedziny analizy, były możliwe dzięki działaniom autorów, które niejednokrotnie opierały się na tej samej bazie danych. Podejmując się przeglądu literatury dotyczącej przeciwdziałania, podział na poszczególne techniki nie jest możliwy z powodu bardzo odmiennych warunków odniesienia eksperymentów. Dla uzupełnienia, oprócz badań nastawionych bezpośrednio na statki bezzałogowe, wspierano się również opracowaniami ogólnymi, które dotyczą analogicznych podsystemów do tych wykorzystywanych w dronach.

4.3.1 Zakłócanie sygnałów nawigacji satelitarnej

Stworzenie bezpiecznych warunków pomiarowych do symulacji wolnej przestrzeni jest możliwe przy wykorzystaniu komory bezodbiciowej, która zapewnia ekranowanie elektromagnetyczne przed czynnikami zewnętrznymi, a jej wnętrze pokryte jest materiałem pochłaniającym energię fal radiowych. Rozmieszczenie wewnątrz tego pomieszczenia laboratoryjnego generatora sygnałów nawigacji satelitarnej Aeroflex GPSG-1000, obiektu badanego oraz stacji zakłóceń pozwala na realizację pomiarów w sposób powtarzalny [134]. Podczas eksperymentów modulowany częstotliwościowo sygnał zakłócający był transmitowany za pomocą anteny kierunkowej w stronę drona DJI Mavic 2 Zoom z krokiem 3 dB, rozpoczynając od mocy -140 dBm. Wpływ sygnału zakłócającego zaczął ujawniać się w okolicy -90 dBm poprzez wzrost wartości parametru niepewności estymacji pozycji, a przy -68 dBm jego wskazanie zostało całkowicie utracone. Odniesienie tych testów do warunków rzeczywistych pokazało, że w przestrzeni otwartej odbiornik GNSS jest jednak bardziej podatny na zakłócenia [135]. Aby utracić wskazanie pozycji, wystarczy wtedy mniejsza moc stacji zakłóceń niż określona w komorze, co jest powodem dodatkowego wpływu ośrodka propagacyjnego związanego z wielodrogowością oraz zniekształceniami jonosferycznymi sygnału oryginalnego z satelitów nawigacyjnych.

Potrzeba uzyskania jednakowych warunków odniesienia może być także rozwiązana poprzez zastąpienie przyrządów laboratoryjnych emulatorem programowym do wytworzenia przebiegu oraz radiem programowalnym do jego fizycznego odtworzenia [136]. W warunkach izolowanych za odbiornik posłużył często wykorzystywany moduł firmy u-blox wraz z oprogramowaniem pozwalającym na monitorowanie indywidualnego poziomu sygnału każdego z satelitów. Wyniki badań laboratoryjnych wykazały, że zastosowanie techniki zaporowej, przestrajanej i świadomej skutkuje utratą zdolności wskazania pozycji przez odbiornik dla odległości do 25 m, w przeciwieństwie do metod impulsowej i punktowej. Pod określeniem świadomego zakłócania autorzy rozumieją strumień losowo generowanych bitów modulowanych w technice BPSK z częstotliwością 1,023 MHz, bez synchronizacji z GNSS, a pod hasłem mocy sygnału stosunek C/N_0 . Przenosząc eksperymenty do środowiska rzeczywistego, oznaczono dla odniesienia efektywny zasięg zakłócania zaporowego jako 18 m, a następnie stwierdzono większą skuteczność techniki przestrajanej i świadomej. W tym miejscu autorzy zauważyli, że dla zakłóceń przestrajanych poziom wskazywanej mocy sygnału dla każdego z satelitów nigdy całkowicie nie znika. Natomiast przy zakłócaniu świadomym moce sygnału poszczególnych satelitów stopniowo maleją w czasie, aż do całkowitego zaniku. Finalnie, sprawdzając podatność na ten tryb działań dronów DJI Spark i Parrot Bebop, nie stwierdzono przewagi żadnej z dwóch technik, a obiekty badane, będąc już w trybie lotu, zawisały bez ruchu lub, gdy zakłócanie odbywało się przed startem, nie podejmowały żadnej dalszej akcji.

Większa grupa obiektów testowanych w środowisku rzeczywistym wykazała nawet różne zachowania w zależności od modelu urządzenia. Drony firmy DJI i Hubsan, w momencie pojawienia się zakłóceń sygnału GNSS, pozostawały w niezmiennym stanie, podczas gdy urządzenia Autel i ZLL natychmiast rozpoczynały procedurę lądowania. W źródłowym opracowaniu [137] testowano metody zakłócania zaporowego AWGN z próbkowaniem 10 MHz oraz świadomego sygnałem BPSK z próbkowaniem 4,092 MHz. Posłużono się przy tym radiem programowalnym z dodatkowym wzmacniaczem mocy i anteną kierunkową. Efektywny zasięg zakłócania zaporowego dla dronów DJI wyniósł 120 m, dla Autel Evo Nano+ 130 m, natomiast modeli Hubsan Zino Mini Pro i ZLL SG 108 nie udało się zakłócić nawet przy 140 metrach. Przy technice świadomej, dla Autel Evo Nano+ zasięg zakłócania zwiększył się do 130 m, a reszta wyników pozostała bez zmian.

Badania terenowe przeprowadzone z użyciem drona DJI Phantom 4 Pro wykazały także, że zasięg zakłócania zależy nie tylko od odległości, ale także od wysokości, na jakiej znajduje się obiekt [138]. Podczas analizy budowy urządzenia autorzy zauważyli miedzianą przekładkę pod ceramiczną anteną GNSS, która zapewne służy jako płaszczyzna odniesienia i może wprowadzać dodatkowe ekranowanie dla sygnału zakłócającego. Podczas eksperymentów zastosowano zakłócanie zaporowe z pasmem 10 MHz, a do układu radia programowalnego ponownie dołączono wzmacniacz mocy oraz antenę kierunkową. W ten sposób wyznaczono maksymalny zasięg zakłócania przy zerowym kącie pomiędzy anteną

nadajnika a dronem, to jest w momencie, gdy obiekt znajdował się na wysokości 1,5 metra i oddalony był o 150 m. Operując na wysokości 50 m, skuteczny zasięg zmniejszył się do 100 m, a kiedy dron znajdował się na wysokości 100 m, nie udawało się go zakłócić nawet przy odległości 50 m. Przytoczone badania wskazują na konieczność analizy wpływu charakterystyki anteny GNSS na estymację zasięgu nadajników zakłócających, co skutkować będzie potrzebą tworzenia modeli warstwowych.

Na przykładzie modułów firmy u-blox szóstej i ósmej generacji, które są także stosowane w dronach, przedstawiono dwie inne metody badania odporności odbiorników na zakłócanie przestrajane [139]. W pierwszej, sygnał ze sprzętowego symulatora sygnału GNSS został analogowo zsumowany z profesjonalnym generatorem zakłóceń o paśmie 18 MHz i po odpowiednim dopasowaniu poziomów mocy podłączono go do wejścia antenowego obu odbiorników po kolei. Dla odbiornika generacji szóstej utrata możliwości wskazywania poprawnej pozycji nastąpiła przy wartości 38 dB JSR i 28 dB-Hz C/N_0 , a dla modułu generacji ósmej przy wartości 39 dB JSR i 32 dB-Hz C/N_0 . W metodzie drugiej wykorzystano programowy generator sygnału GNSS, a zakłócenia zostały cyfrowo nałożone w paśmie 8 MHz. Tak powstały sygnał, za pośrednictwem modułu radiowego, ścieżką analogową dostarczony był do odbiorników. Tym razem punkt odcięcia dla modułu szóstej generacji nastąpił przy wartości 37 dB JSR i 32 dB-Hz C/N_0 , a dla odbiornika generacji ósmej przy wartości 39 dB JSR i 30 dB-Hz C/N_0 . Obie metody oferują podobne wyniki, w kontekście niezbędnego do zapewnienia utraty funkcjonalności parametru JSR, a różnice między odbiornikami zapewne wynikają z różnych algorytmów wewnętrznych.

Kolejną metodą na bezpieczne przeprowadzenie eksperymentów jest wprowadzenie zaburzenia do odbiornika GNSS, sumując w torze analogowym sygnał z prawdziwej anteny z sygnałem generatora zakłóceń [140]. W ten sposób przetestowano zachowanie modułu firmy u-blox dziewiątej generacji w obecności podstawowych technik zakłócania, także w kontekście ewentualnego wykrywania takiej sytuacji na podstawie zarejestrowanej reakcji. Spadki wartości C/N_0 oraz poziomu wzmocnienia toru wejściowego odbiornika dla techniki punktowej i zaporowej były stałe w czasie, w przeciwieństwie do zakłócania przestrajanego, w którym zauważalny jest charakter oscylacyjny. Dodatkowa modyfikacja metody przestrajanej, gdzie wypełnienie sygnału wynosiło 50%, powodowała, zdaniem autorów, że ten typ zakłóceń jest trudniejszy do odróżnienia od naturalnie zmiennego przebiegu parametru C/N_0 .

Technika przestrajana może zostać także użyta do rozszerzenia pola działania stacji zakłóceń na kilka zakresów częstotliwości GNSS [141]. Tym razem cyfrowo wygenerowano sinusoidalną falę zakłócającą, dodano do niej szum o dziesięć razy mniejszej amplitudzie i odtworzono przy pomocy radia programowalnego z częstotliwością próbkowania 2 MHz. Przeskoki częstotliwości następowały z krokiem 1 MHz, a ich zakres pokrywał pasma L1, L2 oraz L5. Badania przeprowadzone w małej skali na odległości 5 m wykazały skuteczność zakłócania zarówno dla modułu u-blox dziewiątej generacji, jak i dla drona DJI FPV

Combo. Zgodnie z obliczeniami autorów, zasięg osiągnięty w powyższym eksperymencie przy mocy nadawania -10 dBm i wzmacnieniu anteny 8 dBi można przeskalować do ponad 2 km przy zwiększeniu mocy do 20 W.

Aspekt oszukiwania pozycji, zamiast całkowitego odcinania odbiornika od jej wskazania, leży poza zakresem tego opracowania. Pierwszym z powodów jest niedawne wyłączenie w oprogramowaniu dronów DJI funkcji wymuszonego blokowania lotów w strefach zastrzeżonych, na imitowaniu których polegał ten rodzaj ataku. Wielu producentów nigdy nie implementowało nawet tej funkcji, gdyż nie udało się stworzyć regulacji prawnych wymuszających automatyczne respektowanie tych barier. Dodatkowo proces oszukiwania jest znacznie bardziej skomplikowany niż zakłócanie, a także powstaje wiele metod obrony przed tą formą ataku [142].

4.3.2 Zakłócanie sygnałów sterowania

Autorskie protokoły komunikacyjne stosowane w komercyjnych statkach bezzałogowych nie stwarzają tak wielu możliwości przeprowadzenia eksperymentów przy pomocy symulacji programowych i emulatorów sygnału rzeczywistego, jak w przypadku dobrze udokumentowanej nawigacji satelitarnej. Stworzenie modelu bazującego na znajomości modulacji, czasu trwania ramki czy interwału przeskoków częstotliwości w technice FHSS jest jednak możliwe i daje ogólny pogląd na porównanie poszczególnych metod zakłócania. Należy jednak spodziewać się, iż mimo zachowania charakteru przebiegu wynikowego i wzajemnych zależności między metodami, proste symulacje mogą wypadać o 5 dB do 10 dB bardziej optymistycznie w kontekście estymacji, niezbędnego do uzyskania danej stopy błędów, stosunku JSR [143].

Dobłą metodą budowy powtarzalnych warunków wydaje się zestawienie połączenia kablowego z odpowiednim poziomem tłumienia pomiędzy kontrolerem a dronem, przy wstrzyknięciu danego sygnału zakłócającego za pomocą sumatora analogowego [143]. Podczas eksperymentów wykorzystano popularne do dzisiaj w modelach RC protokoły FASST (ang. *Futaba Advanced Spread Spectrum Technology*) i ACCST (ang. *Advanced Continuous Channel Shifting Technology*), które są podobne pod względem modulacji do tych używanych w pierwszych generacjach dronów DJI. Podstawą warstwy fizycznej jest tu modulacja GFSK (ang. *Gaussian Frequency Shift Keying*), z dodatkowym rozpraszaniem kodowym i skokami częstotliwości w całym paśmie ISM 2,4 GHz. Dla FASST przeznaczono 36 kanałów rozmieszczonych co 2,048 MHz, a czas trwania ramki wynosi 7 ms. Dla ACCST natomiast dostępnych jest 47 kanałów z odstępami 1,5 MHz, a czas transmisji to 9 ms. W artykule autorzy odnieśli podstawowe techniki do własnej realizacji zakłócania świadomego, która zakładała generowanie sygnału o tych samych parametrach modulacji i rozpraszania kodowego, a także znajomość wzorca przeskoków częstotliwości. Powyższe parametry stanowią jednak często nieosiągalną, bardzo dużą porcję informacji o sygnale

właściwym. Technika zakłócania punktowego, mimo że potrafiła spowodować błędy na pojedynczych kanałach, okazała się całościowo nieskuteczna, gdyż dane wysyłane przez kontroler są powtarzane w każdym skoku częstotliwości. Zarówno podczas badań symulacyjnych, jak i na obiekcie rzeczywistym potwierdzono natomiast wpływ czasu przestrajania na skuteczność procesu zakłócania. Dla obu protokołów optymalna okazała się inna wartość, którą określono jako dziesięć razy większą niż szybkość przeskoków częstotliwości. Finalnie, dla FASST proces skutecznego zakłócenia wyrażony stosunkiem JSR dla techniki z przemiataniem wynosi 10 dB, a dla zaproponowanej metody świadomej 2 dB. Dla ACCST różnica między technikami wynosiła 15 dB. Powyższe wyniki można odnieść do warunków rzeczywistych, zakładając model propagacji wolnej przestrzeni oraz odległość pomiędzy dronem a operatorem jako D . Dla FASST i metody przestrajanej skuteczny zasięg wynosi więc $\frac{1}{3}D$, a dla zaproponowanej techniki $\frac{4}{5}D$. Dla ACCST jest to natomiast odpowiednio $\frac{1}{5}D$ i $\frac{7}{8}D$.

Tożsama metoda badawcza, wykorzystująca połączenie kablem antenowym, została przyjęta w eksperymentach z protokołem AFHDS (ang. *Automatic Frequency Hopping Digital System*), który charakteryzuje się czasem ramki wynoszącym 0,6 ms, 500 kHz kanałem z modulacją GFSK bez rozpraszania kodowego oraz interwałem przeskoku częstotliwości równym 1,48 ms [144]. Pierwsza grupa technik nie zakładała żadnej wiedzy o sygnale i obejmowała zakłócanie zaporowe w paśmie 80 MHz oraz przestrajane z różnym okresem. W grupie drugiej natomiast przyjęto znajomość rozkładu kanałów bez sekwencji przeskoków częstotliwości, toteż zastosowano zakłócanie wielopunktowe, zaporowe i z dopasowaną modulacją równoległą na każdym z kanałów. Rodziny charakterystyk pomiarowych przedstawiono w odniesieniu do poziomu stopy błędów o wartości 50% i 99%, gdzie bardziej interesująco, w kontekście niniejszej pracy, przedstawia się wartość druga. W analizowanych wynikach nie ma bezpośrednio określonego parametru JSR, ale dla uzyskania referencji wystarczające jest traktowanie pomiarów relatywnie do najgorszej metody, jaką okazało się zakłócanie zaporowe w całym paśmie. Zakłócanie przestrajane z częstotliwością 100 kHz, aby osiągnąć tę samą stopę błędów, wymagało mocy zakłócania na porównywalnym poziomie do punktu odniesienia, a zmniejszenie częstotliwości przestrajania do 20 kHz poprawiło ten wynik o 3,5 dB. W grupie posiadającej informacje o konkretnie zajmowanych kanałach najslabiej wypadła metoda wielopunktowego zakłócania na każdej częstotliwości środkowej, ale wciąż osiągnęła wynik lepszy o 5,5 dB od referencji. Najlepszą metodą, z rezultatem 10 dB przewagi nad punktem odniesienia, okazało się przestrajanie z częstotliwością 6 kHz, skacząc w sposób liniowy po znanych kanałach sygnałem z dopasowaną do właściwej modulacją. Dla założenia stopy błędów na poziomie 50% różnica między zakłócaniem zaporowym a proponowanym wzrosła nawet do 12 dB, co skutkuje możliwym czterokrotnym wzrostem zasięgu przy tej samej mocy nadawania.

Jak pokazano w omawianej wcześniej pracy, posiadanie szczątkowej wiedzy o sygnale znacząco poprawia skuteczność zakłócania. Przewidzenie wzorca przeskoków częstotliwości może być możliwe, korzystając ze spektrogramu oraz sieci CNN. Pokazano to na przykładzie dronów DJI Phantom i Skywalker, przy obserwacji okna czasowego o długości 50 ms [145]. W podobnym badaniu na przykładzie dronów DJI Air 2s i DJI Mavic 3 również przeprowadzono analizę wzorca przeskoków przy pomocy sieci CNN, a w oparciu o nią zaproponowano inteligentną technikę zakłócania [146]. Nie przedstawiono szczegółów zastosowanej metody, aczkolwiek odniesiono jej skuteczność, przy tej samej stopie błędów, do metody zaporowej, wskazując na wzrost stosunku JSR o 14 dB. Dodatkowo przeprowadzona symulacja wskazuje, że przy założeniu modelu propagacji w wolnej przestrzeni zaproponowana technika inteligentna będzie miała, przy 1500 metrach dystansu do obiektu zakłócanego, porównywalny poziom skuteczności w stosunku do metody przestrajanej na odległości 400 m. Oba eksperymenty z przewidywaniem wzorca przeskoków dotyczyły czystego widmowo sygnału przy wysokim SNR, a w przestrzeni detekcji znajdował się tylko jeden obiekt, co utrudnia odniesienie tego podejścia do warunków rzeczywistych.

Jak wspomniano w sekcji analizy transmisji stosowanych obecnie w komercyjnych bezzałogowych statkach powietrznych, wiele modeli używa zmodyfikowanych protokołów wywodzących się ze standardu Wi-Fi. Jedną ze znanych modyfikacji jest wyeliminowanie specjalnych potwierdzeń zwrotnych (ang. *acknowledgement*, ACK). Ciekawym sposobem na stworzenie stanowiska testowego dla badania odporności na zakłócenia takich protokołów jest użycie standardowego urządzenia Wi-Fi z rozdzieleniem torów nadawczego i odbiorczego [147]. Dzięki temu urządzenia mogą być połączone kablami antenowymi z kontrolowanym tłumieniem, a zakłócenia mogą być wprowadzane jedynie do toru odbiorczego, bez wpływu na potwierdzenia zwrotne. Podejście to umożliwia przetestowanie wielu ustawień modulacji oraz uzyskanie pełnych statystyk pakietów. Jako referencje wskazano w tym przypadku ustawienia: 11 Mbps DSSS (802.11b) i 9 Mbps OFDM (802.11g), a za miarę skuteczności wybrano spadek przepływności odniesionej do stosunku sygnału do zakłóceń (ang. *signal-to-jamming ratio*, SJR), a więc odwrotność JSR. W kroku pierwszym zbadano odporność modulacji referencyjnych na zakłócenia zaporowe o paśmie 50 MHz oraz sygnał BPSK wypełniony losowymi bitami z przepływnością 50 Msps. Dla modulacji OFDM zanotowano wówczas do 3 dB różnicy między tymi dwiema technikami. Zakłócanie zaporowe okazało się skuteczniejsze, a doprowadzenie parametru przepływności do zera wymagało SJR na poziomie 3,5 dB. Dla DSSS różnica między technikami wynosiła tylko 1 dB, lecz skuteczniejsze okazało się zakłócanie BPSK, a zerowa przepływność wystąpiła dla SJR równego 4,5 dB. W drugim eksperymencie zastosowano tylko zakłócenie zaporowe w trybie impulsowym, a stosunek SJR został dobrany dla obu modulacji tak, aby przy ciągłym nadawaniu komunikacja była zablokowana. Dla utrzymania tej sytuacji okres powtarzania sygnału zakłócającego w obu przypadkach nie mógł być większy niż 1 ms, a wypełnienie musiało wynosić co najmniej 30% dla OFDM i 50% dla DSSS. W kroku

trzecim podjęto próbę przetestowania wpływu zakłócania przestrajanego, jednak z powodu ograniczeń sprzętowych udało się uzyskać minimalny czas przemiatania wynoszący tylko 500 ms, charakteryzujący się skokowym, a nie ciągłym zachowaniem. Wpływ dla obu modulacji zamykał się w spadku przepustowości do około 25% wartości nominalnej. Ciekawą poboczną obserwacją jest natomiast całkowita terminacja połączenia w obu przypadkach dla zakłóceń tonem na częstotliwości środkowej lub tonem odsuniętym od niej o 5 MHz, gdy SJR wynosi 0 dB lub mniej. Może to być oczywiście cecha charakterystyczna danego urządzenia, a kwestie modyfikacji protokołu w komercyjnych statkach bezzałogowych mogły także dotknąć tego aspektu.

Konfiguracja testowa dla modulacji 11 Mbps DSSS (802.11b) i 9 Msps OFDM (802.11g) została odtworzona także w pracy przytoczonej na początku bieżącej sekcji [143]. Mimo że dobrana tam częstotliwość zakłócania przestrajanego dla protokołu FASST wynosiła 1,5 kHz, a dla ACCST 6 kHz, przy zakłócaniu Wi-Fi nie miało to znaczącego wpływu i zdecydowano się na dalsze pomiary przy 3 kHz. Wyraźne oddziaływanie na oba protokoły zaczyna się przy -5 dB JSR, a przy -2 dB stan ten się ustala. Dla DSSS, niezależnie od dalszego zwiększania stosunku JSR, przepustowość stabilizuje się na 1,8 Mbps, podczas gdy w tym samym momencie następuje całkowite odcięcie dla OFDM. Technika zakłócania świadomego, przeniesiona z eksperymentów z protokołem FASST, przy maksymalnym stosunku JSR wynoszącym 20 dB, dała ograniczenie transferu dla DSSS do 2,8 Mbps, a dla OFDM do 3,8 Mbps. Metoda wybrana dla ACCST, natomiast dla tego samego stosunku JSR, dała ograniczenie transferu dla DSSS do 2,8 Mbps, a dla OFDM do 4,1 Mbps. Zastosowanie obu metod świadomych ostatecznie nie wywołało całkowitego zakłócenia.

Przenosząc eksperymenty do środowiska rzeczywistego, można rozważać sytuację, w której dron znajduje się w stałej pozycji względem stacji zakłóceń, a wartością mierzoną jest odległość operatora [137]. Scenariusz ten odnosi się do perymetrycznej ochrony obiektu przed atakiem z bezpiecznej odległości. Aby pokryć cały zakres ISM 2,4 GHz szumem zaporowym, zastosowano pięć układów radia programowalnego o wyjściowej mocy -1,2 dB każdy, wraz z wzmacniaczem mocy 30 dB i anteną kierunkową o wzmacnieniu 18 dBi. Stacja zakłóceń była umieszczona 6 m od badanego obiektu. Najbardziej wrażliwym obiektem okazał się ZLL SG 108, który w odległości 30 m wykazał całkowite zakłócenie i samoczynnie wylądował. W przypadku Autel Evo Nano+ wymagana odległość operatora wzrosła natomiast do 50 m. Modele DJI Mini i DJI Mini 3 Pro zachowywały stabilność do odległości 40 m, a przycięcia obrazu oraz spowolnienie reakcji nasilały się znacznie od 85 m, co utrudniało operacje. Ostatecznie, utrata kontroli nastąpiła na 120 metrach. Ilość sprzętu wykorzystanego przy eksperymentach wydaje się dość znaczna, z uwagi na ograniczenie do 20 MHz pasma zastosowanego układu generatora zakłóceń ADALM-PLUTO, który wymusza pracę kilku jednostek równolegle. Ciekawym rozwiązaniem tego problemu może być sprzętowa modyfikacja kodu oraz przeniesienie systemu zakłóceń z domeny programowej do sprzętowej. Efekt pokrycia tego pasma można uzyskać wtedy dwoma

urządzeniami dwukanałowymi [148].

Zakłócanie zaporowe pojawia się dość często w literaturze jako uniwersalna metoda oddziaływania na statki bezzałogowe. W niektórych opracowaniach niestety nie da się znaleźć dokładnych danych, z których można wnioskować o szerszym kontekście zastosowania. Przykładem jest artykuł przedstawiający wpływ emisji w paśmie ISM 2,4 GHz na połączenie Parrot AR.Drone 2.0 z aplikacją służącą do sterowania [149]. Po aktywacji stacji zakłóceń, która operowała z mocą 0 dBm, zasięg łączności z dronem skrócił się z początkowych 50 m do 9 m. Po dodaniu wzmacniacza do stacji i uzyskaniu mocy 20 dBm wystąpiła dalsza redukcja odległości skutecznego połączenia do 2,5 metra. Nie wiadomo jednak nic o wzmocnieniu anteny ani o położeniu stacji względem obiektów. Ten sam typ zakłóceń wygenerowano, używając zestawu USRP B200 mini, wzmacniacza o mocy 33 dBm i anteny o wzmocnieniu 10 dBi [150]. Obiektami badanymi były tym razem drony DJI Mavic Air, DJI Phantom 4 Pro v2.0 i DJI Mini 2, a testy przeprowadzono w środowisku podmiejskim. Podczas eksperymentów wykazano skuteczność metody, objawiającą się samoczynnym lądowaniem obiektów, które znalazły się w odległości 40 m od stacji. Nieznane jest tu jednak położenie samego operatora, co nie pozwala odnieść wyników do rzeczywistych warunków wtargnięcia obiektu w strefę ochrony. Jak ważny jest to aspekt, obrazuje przykład zastosowania komercyjnego urządzenia zakłócającego VG5W20 o mocy 34 dBm, które wpływa na obiekt DJI Phantom 2 Vision dopiero z odległości około 2 m, kiedy operator oddalony jest o 250 m [151].

Rozdział 5

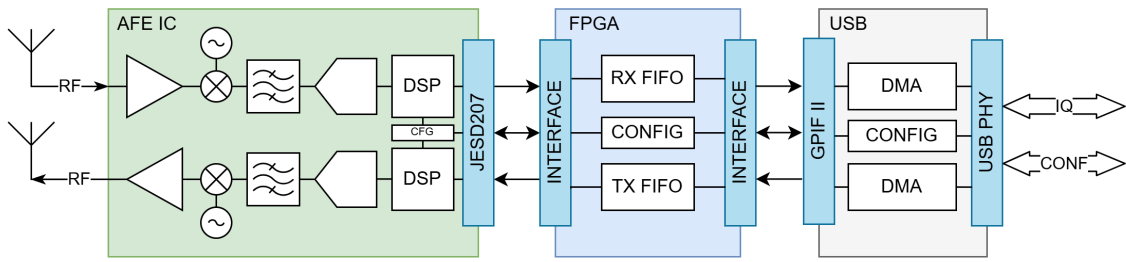
Prototyp sensora i efektora radioelektronicznego

5.1 Koncepcja radia programowalnego

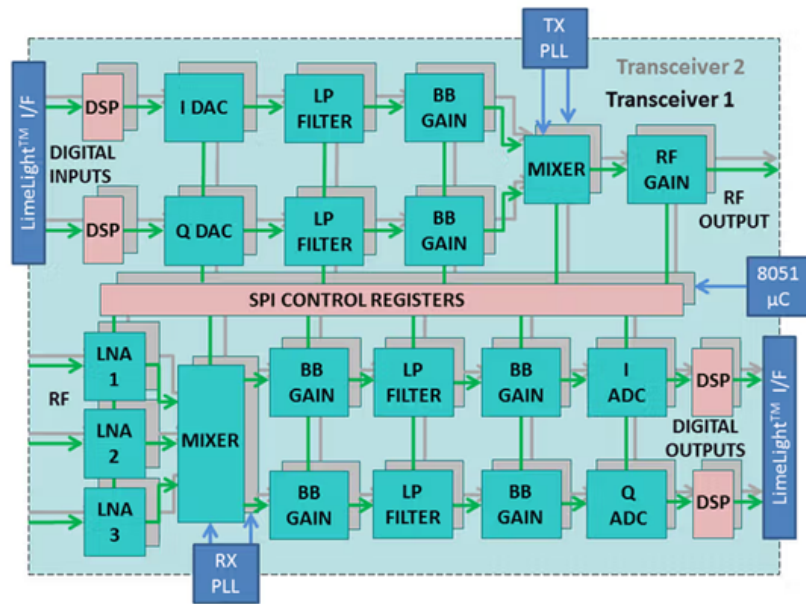
Radio programowe lub, w dosłownym tłumaczeniu, radio definiowane programowo (ang. *Software Defined Radio*, SDR) to concept, który rozwijany był początkowo przez kilka grup badaczy w latach siedemdziesiątych i osiemdziesiątych w Stanach Zjednoczonych. Pierwsza jego fizyczna implementacja powstała w ramach militarnego programu organizowanego przez DARPA (ang. *Defense Advanced Research Projects Agency*) w latach dziewięćdziesiątych. W roku 1992 Joseph Mitola opublikował jedną ze swoich pierwszych prac w tym temacie, a następny ważny krok w rozwoju tej koncepcji stanowiło stworzenie otwartego oprogramowania GNU Radio, oferującego wiele gotowych funkcji do przetwarzania sygnałów. W roku 2009 firma Lime Microsystems wprowadziła do komercyjnej sprzedaży pierwszy układ scalony, który posiadał zintegrowane funkcje niezbędne do realizacji idei radia programowalnego. Od tego czasu wiele innych firm postawiło także na rozwój w kierunku zwiększenia możliwości tej technologii, a radia programowalne zyskały popularność wśród szerokiego grona odbiorców, zarówno profesjonalnych, jak i hobbystycznych [152].

5.1.1 Budowa wewnętrzna

Urządzenia SDR działają w oparciu o architekturę sprzętowo-programową, w której komponent programowy odpowiedzialny jest za przetwarzanie sygnału pasma podstawowego i zastępuje tradycyjne elementy fizyczne, takie jak modulatory, detektory czy filtry. Zarys budowy urządzeń dostępnych na rynku zostanie przedstawiony na podstawie LimeSDR-USB, które stanowi platformę prototypową dla prowadzonego projektu. Główny podział na trzy komponenty, gdzie w tym przypadku każdy z nich stanowi osobny układ scalony (ang. *Integrated Circuit*, IC), zilustrowany jest na rysunku 5.1.



Rysunek 5.1: Architektura modelowego układu SDR firmy Lime Microsystems.



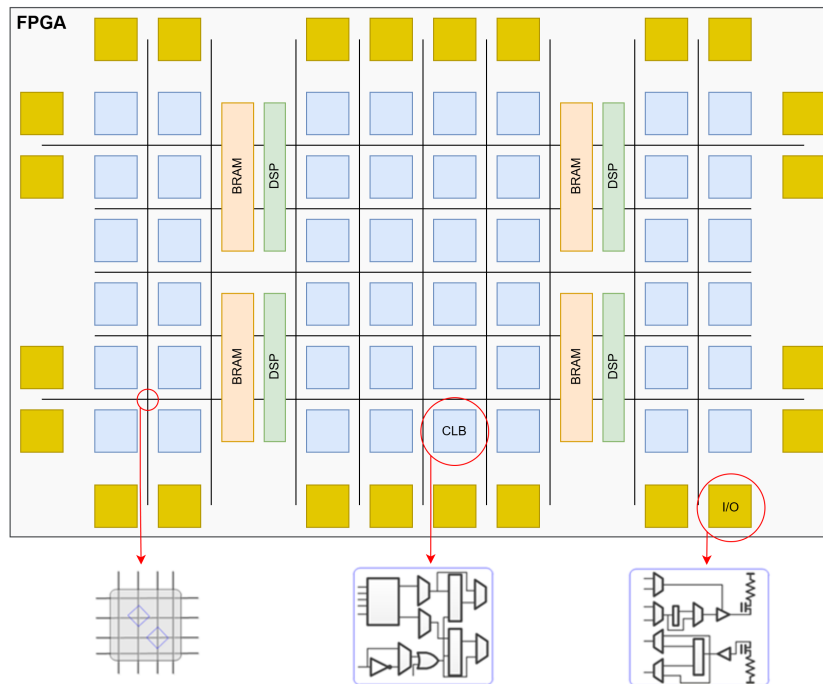
Rysunek 5.2: Budowa wewnętrzna AFE LMS7002M [153].

Najbardziej specyficznym elementem w tej konfiguracji jest właśnie układ końcówki analogowej (ang. *analog front-end*, AFE) LMS7002M [153], który odpowiada za dwukierunkowe konwertowanie sygnałów między domeną cyfrową a analogową. Oprócz przetworników o rozdzielczości 12 bitów, integruje on wzmacniacze wejściowe i wyjściowe, miksery, filtry oraz syntezy częstotliwości, co schematycznie przedstawia rysunek 5.2. Tor odbiorczy oraz nadawczy pracują w trybie przemiany bezpośredniej, zwanym także homodynowym lub trybem z zerową częstotliwością pośrednią (ang. *Zero Intermediate Frequency*, ZIF). Ten typ odbiornika eliminuje kilka problemów spotykanych w układach heterodynowych, ma jednak także swoje wady, takie jak składowe stałe oraz niezrównoważenie amplitudy i fazy sygnałów. Układ AFE zapewnia pewne procesy kalibracyjne, aby minimalizować te niedoskonałości. W konwencji ZIF wykorzystywana jest reprezentacja sygnału polegająca na przedstawieniu go jako kombinacji dwóch, prostopadłych do siebie w fazie składowych. Przyjmuje się, że sygnał kosinusoidalny jest w fazie (ang. *In-phase*, I), a sinusoida jest składową kwadraturową (ang. *Quadrature*, Q), stąd często w opracowaniach dotyczących radia programowalnego używa się określenia strumienia IQ.

Rozpatrując przepływ sygnału w torze nadawczym, to procedura ta rozpoczyna się od dostarczenia strumienia cyfrowych próbek IQ do układu LMS7002M przez interfejs LimeLight, kompatybilny ze standardem JESD207. Próbki są przetwarzane przez konfigurowalne bloki DSP (ang. *Digital Signal Processing*), a następnie dostarczane do wbudowanych przetworników DAC (ang. *Digital Analog Converter*). Tak powstały sygnał analogowy, jeszcze przed wyjściem na zewnątrz układu scalonego, poddawany jest filtracji dolnoprzepustowej oraz wchodzi na mieszacz zasilany przez nadawczą PLL (ang. *Phase Locked Loop*). Zmodulowany sygnał przechodzi jeszcze przez wyjściową kaskadę wzmacniaczy mocy, a następnie opuszcza układ scalony w stronę elementu antenowego.

Rozpatrując przepływ w torze odbiorczym, sygnał przychodzący od strony elementu antenowego najpierw trafia na jeden z trzech LNA (ang. *Low Noise Amplifier*), a następnie, przy pomocy mieszacza zasilanego przez PLL odbiorczą, sprowadzany jest do pasma podstawowego. W kolejnym etapie sekcja wzmacniacza transimpedancyjnego formuje sygnał przed wejściem na dolnoprzepustowy filtr antyaliasingowy. Po filtracji kolejny stopień wzmacniacza programowalnego wprowadza jeszcze korekcję niedoskonałości toru, a sygnał dopasowywany jest do zakresu dynamicznego przetwornika ADC (ang. *Analog Digital Converter*). Potem strumień w postaci cyfrowej trafia już do programowalnego bloku DSP, a następnie jest wystawiany na interfejs LimeLight do procesora pasma podstawowego.

Rolę procesora pasma podstawowego w wykonaniu tym pełni układ FPGA (ang. *Field Programmable Gate Array*) Altera Cyclone IV EP4CE40F23, który charakteryzuje się możliwością konfigurowania struktury wewnętrznej w celu realizacji danej funkcji logicznej. Uogólniona budowa wewnętrzna układów z tej kategorii przedstawiona jest na schemacie 5.3. Podstawową jednostką, z jakiej zbudowane są wewnętrzne zasoby FPGA, jest komórka CLB (ang. *Configurable Logic Block*). Jej budowa zależy od konkretnego wykonania układu, ale zazwyczaj realizacja przez nią funkcji logicznych opiera się na elementach LUT (ang. *Look-Up Table*), multiplekserach i przerzutnikach. Komórki CLB wymieniają informacje między sobą poprzez macierz programowalnych połączeń wewnętrznych, z której część dedykowana jest do rozprowadzania sygnałów zegarowych. Poza logiką wewnętrzną układy FPGA zawierają specjalne komórki wejścia i wyjścia, obsługujące różne standardy elektryczne dla łatwiejszej integracji z układami peryferyjnymi. Nowoczesne wykonania FPGA zawierają także szereg zintegrowanych elementów, takich jak pamięci blokowe (ang. *Block Random Access Memory*, BRAM), generatory sygnału zegarowego oraz komórki DSP. Te o największej skali integracji natomiast wyposażone są w dedykowane kontrolery pamięci, złożone moduły wspomagania obsługi szybkich interfejsów komunikacyjnych czy osadzone rdzenie mikroprocesorów. Mimo ogromnego potencjału, jaki niesie zastosowanie układów tego typu, w dostępnych komercyjnie wykonaniach SDR zapewniają one głównie buforowanie strumieni cyfrowych IQ oraz dopasowanie interfejsów pomiędzy AFE a kontrolerem USB (ang. *Universal Serial Bus*).

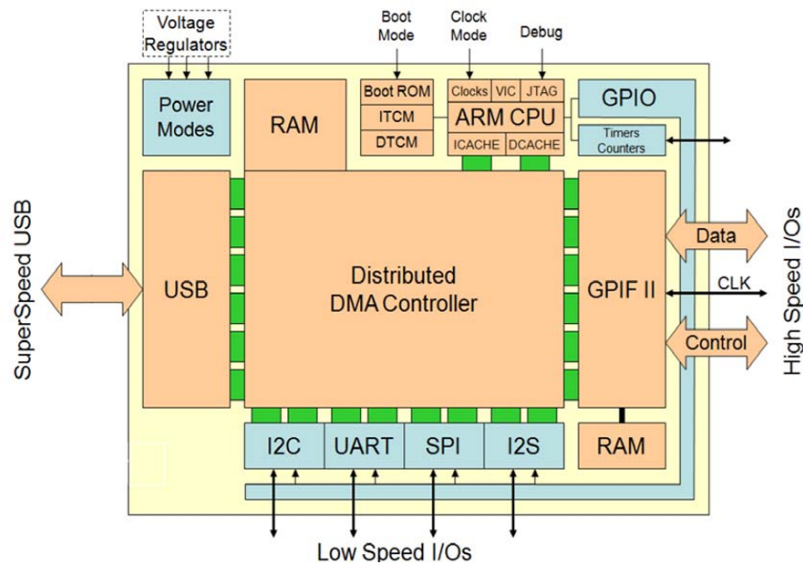


Rysunek 5.3: Budowa wewnętrzna układu FPGA [154].

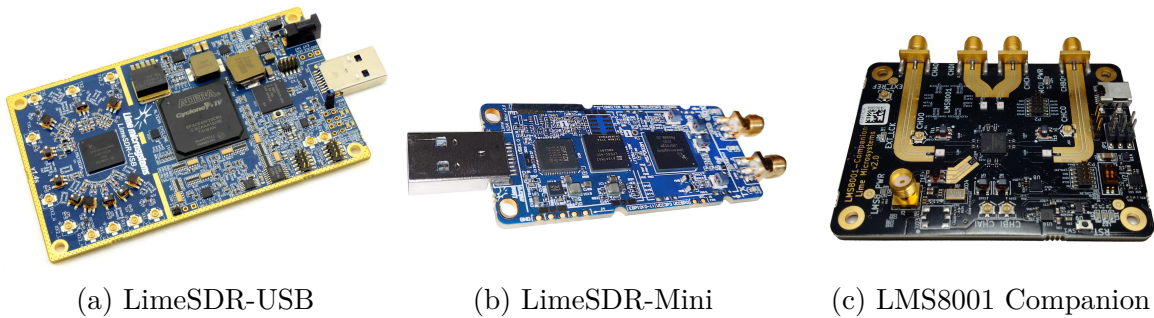
Wymiana danych cyfrowych i komunikatów z urządzeniem końcowym dla opisywanego modułu SDR odbywa się za pomocą interfejsu USB. Dwukierunkowy strumień próbek IQ oraz sterowanie peryferiami trafiają w tym przykładzie do komputera klasy PC (ang. *Personal Computer*), z zachowaniem logicznego rozdzielenia kanałów zgodnego ze sterownikiem w oprogramowaniu końcowym. Zastosowano tutaj zewnętrzny układ scalony, aby zapewnić odpowiednią szybkość przesyłu danych i nie nadwyręzać zasobów logicznych FPGA. Kontroler USB posiada szerokie możliwości konfiguracji, ale nie jest układem programowalnym w kontekście toru radiowego. Jego celem jest przekazywanie danych z równoległych interfejsów do strumienia szeregowego zgodnego z warstwą fizyczną magistrali USB. W tym celu integruje on wewnętrzną jednostkę CPU (ang. *Central Processing Unit*), zasoby RAM (ang. *Random Access Memory*) oraz rozproszony kontroler DMA (ang. *Direct Memory Access*). Jego schematyczna budowa przedstawiona jest na rysunku 5.4. Ta architektura z punktu widzenia kontrolera pozwala na teoretyczny transfer pomiędzy interfejsem GPIF II (ang. *General Programmable Interface*) a USB 3.0 z prędkością 375 MBps. Wydzielony kanał USB 2.0 potrafi także działać równolegle i wspomaga podłączenie urządzeń peryferyjnych operujących na wolniejszych magistralach szeregowych UART (ang. *Universal Asynchronous Receiver-Transmitter*) czy SPI (ang. *Serial Peripheral Interface*).

5.1.2 Porównanie dostępnych urządzeń

Układ kompletnego SDR od firmy Lime Microsystems występuje w kilku wariantach opartych na tej samej opisywanej wcześniej końcówce analogowej. Wersja LimeSDR-USB



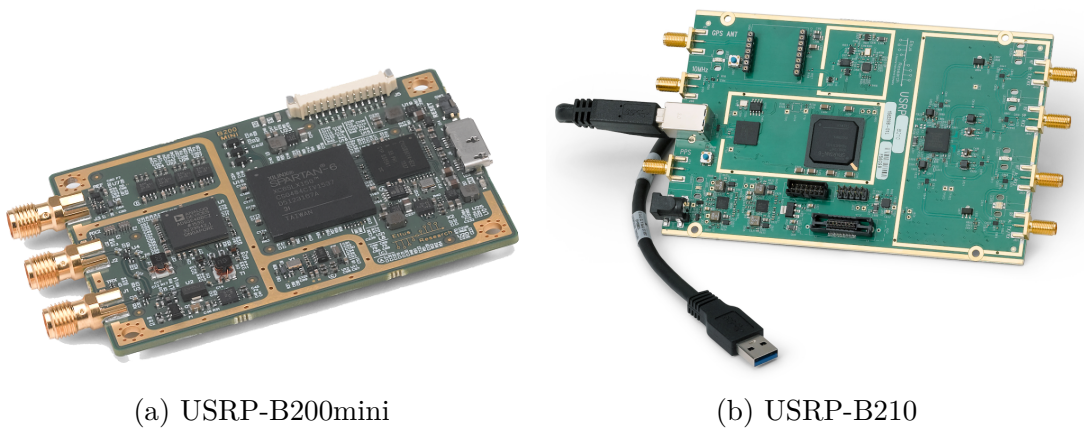
Rysunek 5.4: Budowa wewnętrzna kontrolera SuperSpeed USB FX3 [155].



Rysunek 5.5: Układy z rodziny LimeSDR [153].

oferuje dwa kanały odbiorcze i dwa kanały nadawcze, a wariant LimeSDR-Mini obsługuje fizycznie tylko po jednym wyprowadzeniu dla każdego z nich. Podstawowy zakres częstotliwości pracy obu modułów pozostaje w granicach od 100 kHz do 3.8 GHz i jest rozszerzalny do 10 GHz poprzez specjalną przystawkę towarzyszącą, która bazuje na układzie LMS8001A. Mimo że częstotliwość próbkowania określona w dokumentacji AFE wynosi 96 MHz, producent dla gotowego układu podaje wartości dla LimeSDR-USB 61,44 MHz, a dla wersji LimeSDR-Mini 30,72 MHz [153]. Różnica między osiąganymi tych realizacji spowodowana jest zastosowaniem innego kontrolera USB. Wersja standardowa posiada opisany wcześniej układ scalony FX3 [155], a wersja miniaturowa bazuje na FT601 [156] o gorszych parametrach. Opisywane płyty przedstawia rysunek 5.5.

Modułem, który pojawia się bardzo często podczas analizy literatury w temacie systemów związanych z statkami bezzałogowymi, jest USRP-B210 firmy Ettus Research. W tym przypadku końcówka analogowa oparta jest na układzie scalonym firmy Analog Devices AD9361 i w prezentowanej wersji także posiada dwa tory nadawcze i dwa odbiorcze z przetwornikami o rozdzielczości 12 bitów. W ofercie firmy pozostaje kilka podobnych



(a) USRP-B200mini

(b) USRP-B210

Rysunek 5.6: Układy USRP z serii B [157].

modułów opartych na tym samym układzie scalonym, w tym także takie w wersji miniaturowej z pojedynczymi kanałami. Podstawowy zakres pracy dla tej rodziny pozostaje w granicy od 70 MHz do 6 GHz, a maksymalna częstotliwość próbkowania podobnie określona jest na 61,44 MHz [157]. Wymienione układy również korzystają z wcześniej wspomnianego kontrolera USB FX3, stąd ograniczenia w prędkości transferu są takie same jak dla LimeSDR-USB. Opisywane płyty przedstawione są na rysunku 5.6.

W ostatnich latach coraz częściej w pracach związanych z przetwarzaniem sygnałów dronowych pojawia się także urządzenie o klasie wyższej niż te poprzednio opisywane. Jest to reprezentant odrębnej rodziny firmy Ettus Research, a mianowicie USRP-X310. Tym razem jest to platforma modułowa, a jej parametry zależą od zainstalowanych dwóch niezależnych kart rozszerzeń. W tym wykonaniu możliwe jest osiągnięcie pokrycia zakresu częstotliwości w granicy od 10 MHz do 6 GHz, przy rozdzielczości 14 bitów. Wyróżniającą się dla tej platformy jest zdolność uzyskania pasma natychmiastowego do 160 MHz, co jednak wymaga rezygnacji z interfejsu USB na rzecz podwójnego interfejsu Gigabit Ethernet [157]. Opisywane urządzenie przedstawia rysunek 5.7.

Rozważając wybór modelowej platformy do dalszych prac badawczych, stawiano na dostępność oraz niewielki koszt pojedynczego urządzenia, mając na uwadze potrzebę zastosowania kilku sztuk w finalnym rozwiązaniu. W te kategorie nie wpisywał się układ USRP-X310, który znacznie odbiega od innych modeli z tego porównania. Rozpoczynając prace nad tematem w roku 2021, zdecydowano się na wybór najtańszych platform należących do rodziny LimeSDR. Na ich podstawie budowano dalszą wiedzę o sygnałach dronowych i rozwijano algorytmy zarówno w aspekcie detekcji, jak i neutralizacji. Nie bez znaczenia była także szczegółowa dokumentacja oraz dostępność oprogramowania kontrolnego umożliwiającego nawet ręczne ustawienie każdego rejestru wewnątrz AFE, co jest niespotykane w innych rozwiązaniach. Dostępność otwartych źródeł zarówno dla kodu PC, jak i dla projektu FPGA, w modyfikacji których również zauważalny był pewien



Rysunek 5.7: Urządzenie USRP X310 [157].

potencjał badawczy i wdrozeniowy, dały pełną swobodę w dostosowaniu urządzenia do potrzeb projektu. Dodatkowo w tym samym okresie producent zapowiedział powstanie zmodernizowanej wersji LimeSDR-Mini 2.0 ze zwiększonymi zasobami FPGA, która obecnie w niezmienionym rozmiarze oferuje przestrzeń logiczną porównywalną do LimeSDR-USB. Zastosowanie wypracowanych technik nie ogranicza się jednak tylko do wybranej platformy sprzętowej, a większość z proponowanych algorytmów jest uniwersalna i z powodzeniem przeniesiona może zostać na inne modele.

5.1.3 Oprogramowanie obsługowe

Konfiguracja poprawnej wymiany strumienia próbek pomiędzy końcówką analogową a aplikacją użytkownika jest zadaniem wymagającym ustawienia wielu parametrów części sprzętowej. Oprogramowanie dostarczane przez producenta LimeSDR o nazwie LimeSuite jest dedykowane do platform zawierających układ AFE LMS7002M. Producent zapewnia pełny dostęp do źródeł oraz skompilowaną aplikację z interfejsem graficznym, w której wyświetlany jest strumień IQ w dziedzinie czasu i częstotliwości. Aplikacja pozwala na zapisanie strumienia w pliku tekstowym oraz odtworzenie wcześniej przygotowanego przebiegu. Daje też możliwość aktualizacji oprogramowania części sprzętowej i przeprowadzenia procesów kalibracyjnych. Wiele parametrów dostępnych jest z poziomu interfejsu graficznego, ale oprócz tego producent zapewnił ścieżkę do manualnego ustawienia dowolnego rejestru z przestrzeni adresowej AFE. Poza tym dostępne jest również API (ang. *Application Programming Interface*), wraz z przykładami nadawania i odbierania próbek z poziomu C++ oraz Pythona, które pozwala na wykorzystanie dowolnych bibliotek z przestrzeni

tych języków oraz wprowadzenie własnych optymalizacji.

GNU Radio natomiast to platforma cyfrowego przetwarzania sygnałów, która nie jest nastawiona na obsługę konkretnego modułu SDR. Konfiguracja w tym przypadku odbywa się na wysokim poziomie abstrakcji i sprowadza się głównie do ustawienia pasma, częstotliwości próbkowania, częstotliwości środkowej czy wzmocnienia. Struktura oprogramowania pozwala zarówno na wykonywanie symulacji, jak i budowanie w sposób graficzny łańcuchów przetwarzania sygnałów we współpracy z urządzeniami fizycznymi. Oprogramowanie również ma charakter otwarty i bardzo szerokie grono osób aktywnie działających przy jego rozwoju. Ponadto zawiera w sobie obszerną bibliotekę gotowych bloków, takich jak: filtry, synchronizatory, modulatory i demodulatory. Każdy blok realizuje funkcję, która w pewien sposób konwertuje wektory wejściowe na wyjściowe, a grafy przepływu ułatwiają projektowanie złożonych algorytmów przetwarzania w sposób modułowy i skalowalny. Mimo dobrej optymalizacji, aplikacja nastawiona jest głównie na modelowanie systemów komunikacyjnych, a szerokopasmowa i wielowątkowa analiza sygnałów w czasie rzeczywistym może spotkać się z pewnymi ograniczeniami wydajności.

Osobną kategorię stanowi oprogramowanie komercyjne typu LabView oraz Matlab. Są to potężne narzędzia do modelowania skomplikowanych algorytmów, które posiadają również biblioteki komunikacyjne do sterowania SDR. Z uwagi na optymalizację urządzenia finalnego w kierunku zastosowania komputera wbudowanego, pozostają one poza obszarem zainteresowania dla wykonania prototypu sensora i efektora. Środowisko Matlab natomiast posłuży w dalszej części do modelowania warunków propagacyjnych oraz symulacji podatności na zakłócenia protokołu radiowego 802.11n.

5.2 Modyfikacje funkcjonalne klasycznego SDR

Architektura programowalna modelowego układu FPGA opiera się na procesach potokowych (ang. *pipeline*) polegających na podziale zadań na specjalizowane grupy. Grupy połączone są ze sobą za pomocą kolejek FIFO (ang. *First In First Out*) w sposób sekwencyjny, a każda z nich wykonuje część zadania. W oryginalnym oprogramowaniu modelowego SDR nie można mówić w tym procesie o przetwarzaniu sygnałów. Próbkę o rozmiarze 12 bitów dla składowej I oraz 12 bitów dla składowej Q są przenoszone pomiędzy interfejsami zgodnymi z AFE oraz z kontrolerem USB. Zadanie FPGA ogranicza się do implementacji maszyn stanów odpowiadających za komunikację z poszczególnymi interfejsami oraz opakowywanie lub rozpakowywanie danych pakietowych, bez wpływu na zawartość strumienia IQ. Całość projektu dostępna jest w postaci otwartych źródeł oraz stworzona została przy użyciu języka VHDL (ang. *Very High Speed Integrated Circuit Hardware Description Language*). W strukturze wewnętrznej FPGA zawarty jest także procesor ogólnego przeznaczenia NIOS II, który obsługuje zdarzenia wymagające implementacji pętli o zmiennej długości czy instrukcje warunkowe. W opisywanym przypadku odpowiada on za wymianę

komunikatów z komputerem PC i wysterowanie AFE poprzez interfejs szeregowy zgodnie z poleceniami aplikacji użytkownika. Kiedy proces transferu próbek zostanie zestawiony, a nowe komendy nie płyną, procesor nie wykonuje żadnej funkcji. Jego oprogramowanie napisane jest w języku C i w pracach nad prototypem nie było modyfikowane.

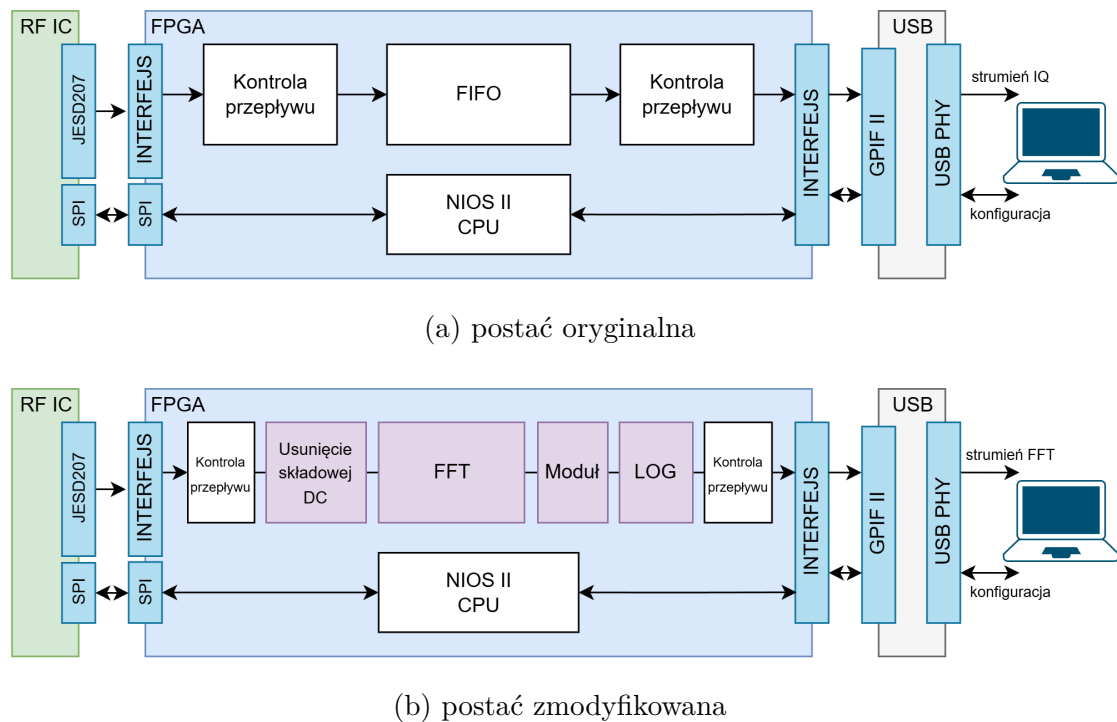
5.2.1 Wykorzystanie pełnej częstotliwości próbkowania

Wykonując pierwsze obserwacje sygnałów dronowych i chcąc zachować dla późniejszej analizy jak największy wycinek pasma pomiędzy 2,4000 GHz a 2,4835 GHz, porównywane urządzenia LimeSDR-USB oraz USRP-B210 nie dawały stabilnego przepływu strumienia IQ przy maksymalnej częstotliwości próbkowania określonej na 61,44 MHz. Zjawisko odrzucania pakietów, na przykład z powodu przepełnienia buforów sprzętowych, jest zjawiskiem znanym, gdyż komunikacja pomiędzy SDR a PC nie przewiduje retransmisji danych. Dodatkowo oferowane przez wymienione układy pasmo nie zapewnia pełnego pokrycia zakresu częstotliwości ISM 2,4 GHz, w którym należy poszukiwać sygnałów komercyjnych statków bezzałogowych. Rozwiązaniem tego problemu w kilku opracowaniach było zastosowanie dwóch urządzeń i podział pasma na część górną i dolną. Nie rozwiązywało to problemu strat pakietów, choć niektóre metody detekcji były na to odporne, traktując obraz całego spektrum w bardzo ogólny sposób. Dla technik bazujących natomiast na parametrach statystycznych, uwzględniających na przykład czas trwania ramki, mogło to powodować błędy klasyfikacji.

Istota w ograniczeniach związanych z transferem wynika w pierwszej kolejności z teoretycznej przepustowości, jaką można uzyskać poprzez kontroler USB 3.0, określonej przez producenta na 375 MBps. Transfer strumienia dla dwóch kanałów zawierających dwa razy po 12 bitów próbek IQ daje wymaganą prędkość przepływu na poziomie 368,64 MBps dla surowych danych. Wartość ta jest blisko wyznaczonej granicy i nie uwzględnia jeszcze narzutu protokołu. Po zestawieniu strumienia, nawet wysłanie pojedynczej komendy w kanale sterowania interfejsu USB może zaburzyć ten transfer, dlatego większość aplikacji sterujących wstrzymuje przepływ danych przy dynamicznej zmianie parametrów AFE. Opisane w tej sekcji modyfikacje są przedmiotem pierwszej autorskiej publikacji [15].

5.2.2 Wsparcie sprzętowe obliczeń FFT

Poza dużą prędkością przesyłu pomiędzy SDR a PC niezbędną do zobrazowania szerokiego pasma, kolejnym aspektem jest potrzeba przetworzenia takiej ilości danych w czasie zbliżonym do rzeczywistego. Po wykonaniu przeglądu literaturowego i badań wstępnych zdecydowano się na dalszy rozwój metod detekcji w oparciu o zapis czasowo-częstotliwościowy, gdzie pierwszym krokiem jest obliczenie FFT. Oryginalne oprogramowanie LimeSDR-USB posiadało w FPGA wolne zasoby logiczne i pozostawiało przestrzeń na implementację dodatkowego łańcucha przetwarzania sygnałów wykonującego tę trans-



Rysunek 5.8: Schemat blokowy zmian architektury FPGA wewnątrz układu SDR, na przykładzie toru odbiorczego.

formację. W budowie ciągu przetwarzania zachowano potokową architekturę, dzięki czemu próbki po początkowym drobnym opóźnieniu, potrzebnym na wypełnienie potoku, trafiają w sposób ciągły do komputera PC już w postaci transformaty. Jej długość początkowo była konfigurowalna, a jej finalny kształt został ustalony na drodze dalszych eksperymentów. Poza zyskiem wynikającym z odciążenia komputera PC z obliczania FFT uzyskano możliwość alokacji pasma USB w bardziej kontrolowany sposób. Zamiast wysyłania strumienia o sumarycznym rozmiarze dla pary IQ wynoszącym 24 bity, można wysłać gotowy wynik transformaty z zdefiniowaną precyzją. Aby nie zmieniać sterowników po stronie aplikacji użytkownika, zdecydowano się na pozostawienie pierwotnego formatu słowa bitowego. Po stronie aplikacji, zamiast widzieć równolegle pary próbek I oraz Q, zaczęto odbierać dwie kolejne wartości estymaty widma. Po tej modyfikacji można przesłać więc dwa razy szerszy obraz pasma w dziedzinie częstotliwości, czyli 122,88 MHz, zachowując pierwotne wypełnienie łącza USB. Maksymalna częstotliwość próbkowania AFE to jednak 96 MHz, więc finalnie wymagana wartość transferu zmniejszyła się do 288 MBps, a co za tym idzie, stopa błędów przesyłu została zminimalizowana i uzyskano pełne obrazowanie pasma ISM 2,4 GHz przy pomocy jednego urządzenia. Zmiany w strukturze wewnętrznej FPGA pokazane są na schemacie blokowym 5.8.

Tor przetwarzania sygnału rozpoczyna się od wypełnienia wejściowego FIFO próbkami IQ w liczbie odpowiadającej długości FFT. W tym momencie często na zbiór wejściowy nakładana jest złożona funkcja okna, aby zmniejszyć przeciek widmowy. Tutaj jednak

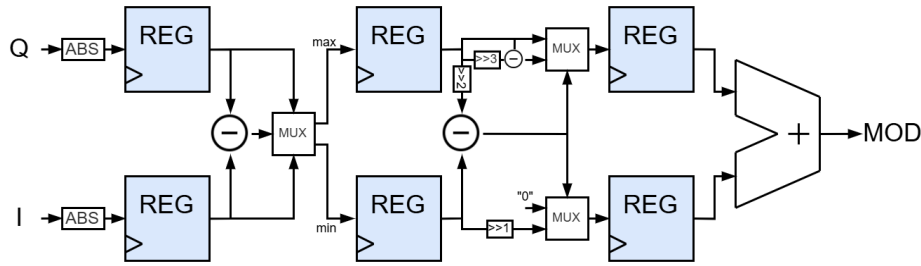
stłumienie sygnału na brzegach okna mogłoby spowodować utratę pewnych istotnych informacji o nim, więc zdecydowano się jedynie na proste okno o kształcie prostokątnym. Takie podejście nadaje się szczególnie do obserwacji sygnałów w stanach przejściowych (ang. *transient*) oraz nie wymaga stosowania współczynników korekcji amplitudy ani energii, co upraszcza analizę [158]. Mając na uwadze powyższe, na tym etapie usuwana ze zbioru próbek jest tylko składowa stała, aby zminimalizować wartość zerowego prążka w widmie. Przygotowane próbki z wyjścia z FIFO przechodzą następnie do modułu kalkulacji FFT. Zastosowano tutaj arytmetykę stałoprzecinkową, a sam moduł obliczania transformaty również pracuje w trybie kwadraturowym. Wejściowe strumienie 12-bitowych próbek IQ generują dwa 24-bitowe strumienie wyjściowe, z uwagi na operacje mnożeń wewnątrz struktury FFT. Aby zapewnić większą rozdzielczość czasową finalnego spektrogramu, zaimplementowano dwa równoległe kanały opisanego powyżej toru przetwarzania, gdzie na jeden z nich kierowane są próbki bezpośrednio z wejścia, a na drugi te opóźnione przez FIFO o długości połowy FFT. W ten sposób można uzyskać efekt zazębiania się transformat (ang. *overlapping*) na poziomie 50%, pomocny przy analizie sygnałów szybko zmiennych.

5.2.3 Metody aproksymacyjne dostosowane do FPGA

Obliczenie w strukturze FPGA modułu liczby zespolonej w sposób bezpośredni, jako pierwiastka z sumy kwadratów I oraz Q, wymaga sporych zasobów logicznych. Tak jak w całym systemie, należało zastosować tu konwencje przetwarzania potokowego z częstotliwością co najmniej 96 MHz. Arytmetyka aproksymacyjna może znacznie uprościć ten proces w zastosowaniach takich jak rozpoznawanie wzorców czy analiza przy pomocy technik uczenia maszynowego [159], a podstawowym wyznacznikiem przy wyborze konkretnego algorytmu przybliżania pierwiastka kwadratowego jest kompromis pomiędzy szybkością a dokładnością. Dodatkowo implementacja powinna być dostosowana do warunków FPGA i obliczeń stałoprzecinkowych, zawierać niewiele kroków oraz nie angażować znaczących zasobów bloków DSP. Przy wstępnej selekcji odpadły więc metody oparte na algorytmach CORDIC (ang. *Coordinate Rotation Digital Computer*) [160] oraz podejściu Newtona-Rapsona [161].

Szczególny przypadek, jakim jest obliczanie pierwiastka z sumy kwadratów dwóch liczb, można aproksymować także poprzez zastosowanie algorytmu o nazwie 'alpha max beta min'. Metoda ta nie jest iteracyjna, ale wymaga w pierwszym kroku porównania wartości bezwzględnych części rzeczywistej i części urojonej liczby zespolonej, aby określić, która z nich jest większa. W kroku drugim natomiast wykonywane są dwa mnożenia przez stałą oraz jedno sumowanie dla podstawowej wersji algorytmu zgodnie z zależnością 5.1:

$$M = \sqrt{I^2 + Q^2} \approx \alpha \max(I, Q) + \beta \min(I, Q). \quad (5.1)$$



Rysunek 5.9: Schemat blokowy elementu wyliczającego aproksymację modułu liczby zespolonej na podstawie zależności 5.2.

Przy założeniu współczynników $\alpha=0,9604$ oraz $\beta=0,3978$ można uzyskać maksymalny błąd aproksymacji na poziomie 3,95%. Dopasowując współczynniki do obliczeń wewnątrz FPGA, zastępując mnożenia operacjami przesunięć bitowych i dodawaniem, dla przyjętych $\alpha = \frac{15}{16}$ i $\beta = \frac{15}{32}$, błąd maksymalny zwiększa się do 6,25%. Ulepszona wersja algorytmu oferuje zmniejszenie tego błędu poprzez wykonanie dodatkowej operacji przyporządkowania do regionu aproksymacji i w zależności od tego, zastosowanie innych współczynników. Przy wykorzystaniu czterech regionów aproksymacji błąd maksymalny może być zmniejszony nawet do 0,24%, ale realizacja sprzętowa w tym podejściu wymaga sześciu bloków DSP dla wykonania operacji mnożenia [162]. Finalnie, z uwagi na ograniczone zasoby FPGA, wybrano rozwiązanie nie wymagające stosowania tych operacji, co pozwoliło na osiągnięcie błędu maksymalnego nieprzekraczającego 3,0% a błędu średniego na poziomie 0,95% [161]. Podejście to opisane jest zależnością 5.2:

$$\alpha, \beta = \begin{cases} \alpha = \frac{7}{8}, \beta = \frac{1}{2} & \text{dla } \min(a, b) > \frac{1}{4} \max(a, b), \\ \alpha = 1, \beta = 0 & \text{dla reszty.} \end{cases} \quad (5.2)$$

Realizacja sprzętowa zależności 5.2 przedstawiona jest na rysunku 5.9. Składa się ona z trzech stopni przetwarzania potokowego rozdzielonych rejestrami (ang. *register*, REG). W kroku pierwszym wyznaczane są wartości bezwzględne składników I oraz Q (ang. *absolute value*, ABS). Następnie poprzez określenie znaku z operacji odejmowania następuje przypisanie części maksymalnej i minimalnej do odpowiedniego toru przy zastosowaniu multipleksera (ang. *multiplexer*, MUX). Tam wykonywane jest mnożenie przez współczynnik, które w przypadku składowej minimalnej sprowadza się do przesunięcia bitowego o jedną pozycję w prawo, a dla składowej maksymalnej do odjęcia jednej ósmej własnej wartości. Kolejny zestaw multiplekserów przekazuje do finalnego stopnia sumacyjnego odpowiednią parę wartości w zależności od znaku operacji $\frac{max}{4} - min$ określającego warunek doboru współczynników.

Zapis obrazu widma w skali decybelowej jest bardzo często używaną formą reprezentacji, pozwalającą na porównanie i interpretację sygnałów o dużym zakresie zmienności. Wyliczona wcześniej aproksymacja modułu liczby zespolonej, zanim zostanie przesłana

do komputera PC, może być przekształcona do tej formy jeszcze na warstwie sprzętowej. Dzięki temu zamiast 24-bitowej wartości w skali liniowej, przesyłamy 4-bitową część całkowitą i 8-bitową część ułamkową, pozostając przy słowie o długości 12 bitów. Korzystamy przy tym z zależności określającej przejście pomiędzy skalą liniową a decybelową dla modułu liczby zespolonej M 5.3:

$$10 \log_{10} M^2 = \frac{20 \log_2 M}{\log_2 10} \approx 6,02 \log_2 M. \quad (5.3)$$

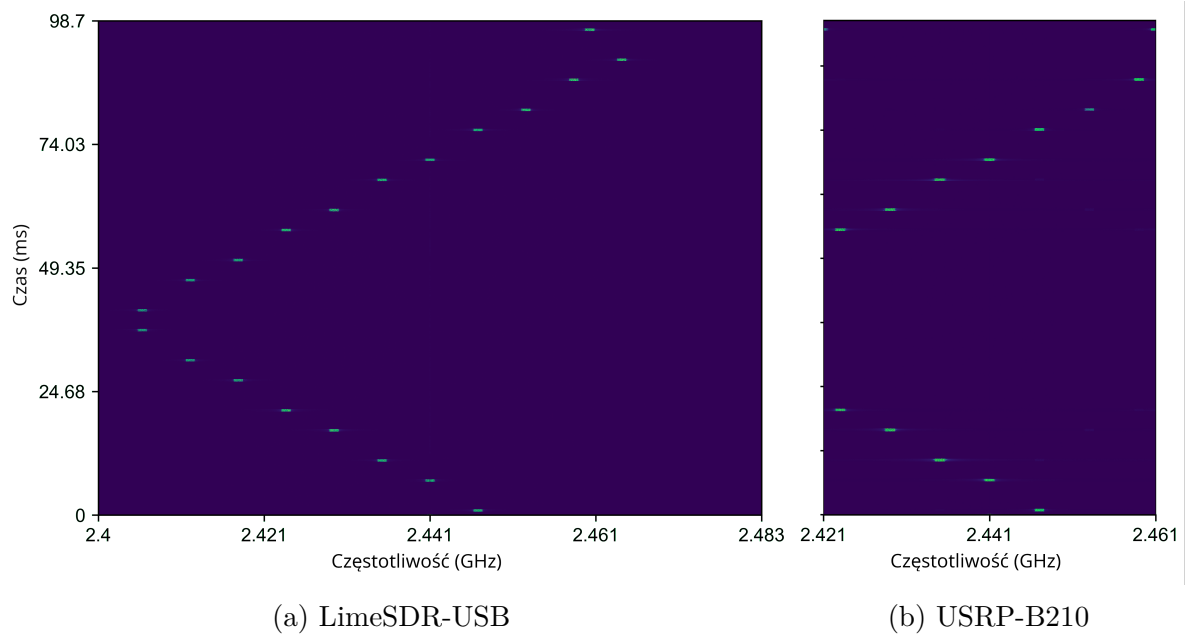
Obliczanie logarytmu w strukturze FPGA w sposób bezpośredni niesie za sobą podobne problemy jak w przypadku pierwiastka w etapie poprzednim. Stosowanie metod aproksymacji odcinkowej i podział operacji na 15 segmentów pozwala na osiągnięcie nawet średniego błędu na poziomie $1,2 \times 10^{-4}$ przy wykorzystaniu 12-bitowej dokładności części ułamkowej [163]. W przypadku przeznaczenia na tę część 8 bitów, dokładność rzędu $3,9 \times 10^{-3}$ jest wystarczająca, dzięki czemu można zmniejszyć liczbę przedziałów aproksymacji.

Metoda dostosowana do obliczeń w sprzęcie w tym przypadku zawiera podział na 4 odcinki, a współczynniki ponownie obliczane są tylko poprzez przesunięcia bitowe [164]. Wybrana technika zapewnia średni błąd aproksymacji na poziomie $2,5 \times 10^{-3}$, co znajduje się poniżej założonej rozdzielczości. Przyszłościowo to samo podejście pozwala zmniejszyć ten błąd nawet do $9,8 \times 10^{-5}$, po wprowadzeniu korekcji zapisem tablicowym. Aproksymację fundamentalnej funkcji $L_a = \log_2(1 + x)$ można zapisać jako 5.4:

$$L_a \approx \begin{cases} (2^0 + 2^{-2} + 2^{-5})x + 0,005 & \text{dla } 0,00 \leq x < 0,25; \\ (2^0 + 2^{-5})x + 0,0684 & \text{dla } 0,25 \leq x < 0,50; \\ (2^{-1} + 2^{-1} + 2^{-3})x + 0,1505 & \text{dla } 0,50 \leq x < 0,75; \\ (2^{-1} + 2^{-2})x + 0,248 & \text{dla } 0,75 \leq x < 1. \end{cases} \quad (5.4)$$

Realizacja sprzętowa zależności 5.4 przedstawiona jest na rysunku 5.10. Proces aproksymacji rozpoczyna się od wyznaczenia wiodącej jedynki (ang. *Leading-One Detector*, LOD) w słowie wejściowym i zakodowania jej w zapisie 1 z N. Następnie kombinacyjny enkoder priorytetowy przetwarza zapis z jedną gorącą jedynką na 4-bitową wartość, która stanowi już gotową część całkowitą wyniku. Ta wartość pobudza przesuwnik beczkowy, który umożliwia rotacje słowa wejściowego o określoną liczbę bitów bez użycia logiki sekwencyjnej. Dwa najstarsze bity po przesunięciu adresują multipleksery, aby z powstałych sum utworzyć odpowiednią dla przedziału część ułamkową aproksymacji. W ostatnim etapie do części ułamkowej może zostać jeszcze dodana korekcja tablicowa.





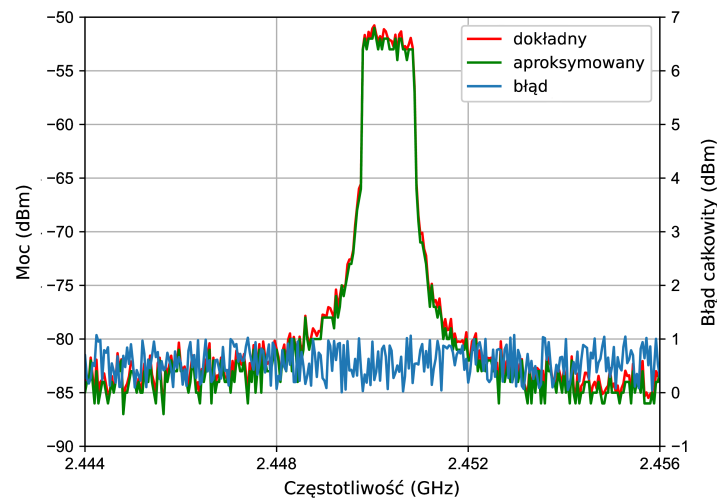
Rysunek 5.11: Przykładowe spektrogramy pozyskane z sygnałów dostarczonych przez badane urządzenia.

pasma ISM 2,4 GHz przy pomocy jednego urządzenia bez strat pakietów. Niezależnie obsłużony jest tor nadawczy, który po aktywacji transmisji danego typu fali zakłócającej nie wymaga dalszej kontroli ze strony oprogramowania wyższego poziomu.

Przykładowy spektrogram przedstawiający zapis radiowej komunikacji aparatury sterującej z dronem DJI Mavic 2 Zoom, pozyskany drogą rozdzielania odbieranego analogowego sygnału antenowego pomiędzy zmodyfikowanym LimeSDR-USB a USRP-B210, przedstawia rysunek 5.11. Dane z prototypu sensora prezentowane są bezpośrednio, a na zapisie pozyskanym z USRP-B210 obliczono FFT w sposób programowy.

Ten sam sygnał referencyjny zbadano pod kątem skumulowanego wpływu zaadaptowanych technik aproksymacji. W tym eksperymencie strumień IQ przed wejściem do modułu estymatora widma wewnątrz FPGA został dodatkowo zachowany w pamięci urządzenia. Następnie przeprowadzono na nim tożsame operacje, nie stosując jednak technik aproksymacyjnych, i porównano z sygnałem wyjściowym dostarczonym przez prototyp sensora. Rysunek 5.12 przedstawia zestawienie przebiegów po zastosowaniu uśrednienia w szesnastu kolejnych wektorach wyjściowych. Zaobserwowany całkowity błąd między dokładnym a przybliżonym widmem z LimeSDR-USB spełnia obecne oczekiwania, nie przekraczając znacznie 1 dB.

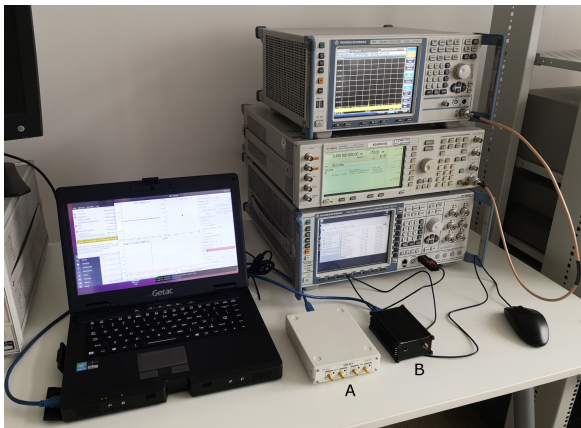
Studium literaturowe przeprowadzone w zakresie detekcji sygnałów dronowych przy pomocy spektrogramu i metod uczenia maszynowego wykazało, iż poziom SNR równy -10 dB może być traktowany jako granica wysokiej skuteczności wielu algorytmów. Stnowisko laboratoryjne zbudowane dla wyznaczenia mocy sygnału odbiornika, niezbędnej do uzyskania danego SNR dla urządzenia referencyjnego i wykonanego prototypu, przed-



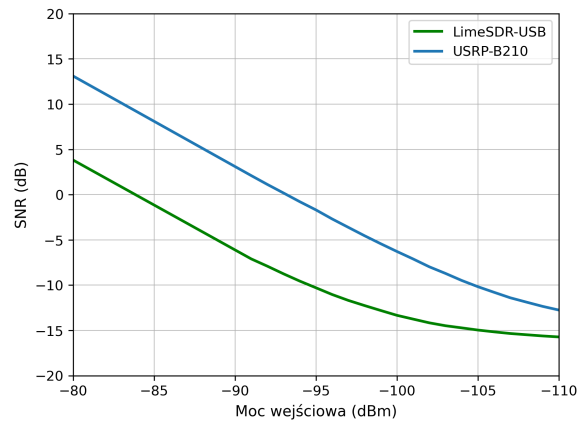
Rysunek 5.12: Zapis pojedynczej ramki transmisji danych drona w dziedzinie częstotliwości, przy użyciu dokładnych i przybliżonych technik oraz całkowity błąd przybliżenia.

stawia rysunek 5.13a. Dla zapewnienia powtarzalnych warunków przy badaniach, tym razem sygnał antenowy zastąpiono sygnałem z urządzenia laboratoryjnego. Generator cyfrowy Agilent E4432B podłączony został przewodem o niskich stratach, w pierwszej kolejności do zmodyfikowanego LimeSDR-USB, a następnie do USRP-B210. Urządzenia pozostawały włączone przez 2 godziny przed rozpoczęciem pomiarów w celu uzyskania równowagi termicznej, a rzeczywisty poziom sygnału na wejściu SDR został potwierdzony pomiarem przez analizator Rohde&Schwarz FSV. Oba badane urządzenia operowały na maksymalnym wzmocnieniu toru analogowego, a jako sygnał wzorcowy wybrano transmisję z modulacją GFSK w zakresie ISM 2,4 GHz z pasmem 2 MHz. Podczas eksperymentów zapisano próbki pozwalające na wyliczenie 1000 wartości SNR dla każdego poziomu sygnału wejściowego zmienianego w zakresie od -80 dBm do -120 dBm z krokiem 1 dBm. Finalna wartość SNR dla danego kroku określona została statystycznie przy zastosowaniu metody MLE (ang. *Maximum Likelihood Estimation*). Porównanie zaprezentowane na rysunku 5.13b wskazuje na około 9,5 dB różnicy pomiędzy obliczonym SNR a mocą sygnału wejściowego, zestawiając liniowe zakresy pomiarowe obu urządzeń. Spowodowane jest to mniejszym dostępnym wzmocnieniem toru analogowego LimeSDR-USB, większym współczynnikiem szumów wejściowych, a także ponad dwukrotnie rozszerzonym pasmem obserwacji. Założona wartość SNR równa -10 dB osiągalna jest w założonych warunkach dla zmodyfikowanego LimeSDR-USB przy mocy wejściowej około -95 dBm, a dla USRP-B210 przy około -105 dBm.

Pomiary toru nadawczego w kontekście wykorzystania w zakłócaniu sygnałów bezzałogowych statków powietrznych wykonane zostały w celu określenia przyszłego zasięgu prototypu oraz potencjalnej konieczności zastosowania zewnętrznego toru analogowego. W tym celu układ LimeSDR-USB połączony został kablem koncentrycznym bezpośrednio



(a)



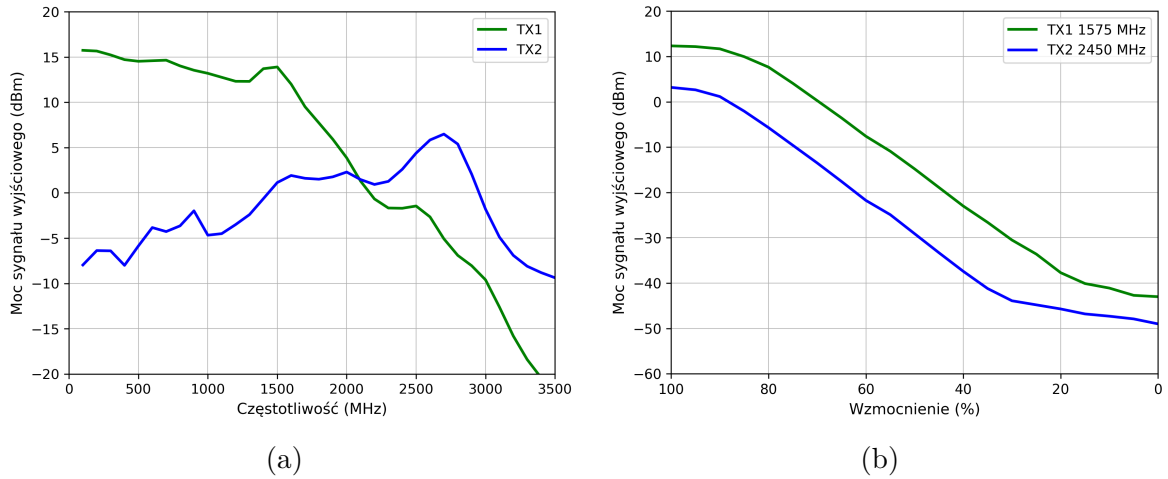
(b)

Rysunek 5.13: Porównanie prototypu z urządzeniem referencyjnym w kontekście niezbędnej mocy sygnału wejściowego dla osiągnięcia danego SNR: (a) stanowisko pomiarowe, (b) zestawienie wyników.

z szerokopasmowym detektorem mocy Agilent U2000A, a kształt generowanego przebiegu zweryfikowany został wcześniej za pomocą analizatora Agilent FieldFox N9912A. Każdy kanał nadawczy SDR posiada po dwa wyjścia przeznaczone do wysokich i niskich częstotliwości, a dla znalezienia najlepszego dopasowania do przeznaczonych celów pomiary wykonano dla każdego z nich, uwzględniając pełny zakres przestrajania. Badania dostępnej mocy wyjściowej w zależności od częstotliwości wykonano dla pojedynczego tonu, co zaprezentowane zostało na wykresie 5.14a. Punkt przecięcia się charakterystyk występuje w okolicy 2100 MHz, a więc dla uzyskania większej mocy zakłócania zakresu związanego z GNSS wybrano tor pierwszy, a dla zakłócania pasma ISM 2,4 GHz tor drugi. Dodatkowo, na wykresie 5.14b, przedstawiono zależność sterowania mocą wyjściową z poziomu dostępnych cyfrowo parametrów końcówki analogowej dla dwóch głównych częstotliwości zakłócania. Oprogramowanie w aplikacji użytkownika pozwala w prosty sposób sterować wzmocnieniem, za pomocą jednej znormalizowanej wartości. W zakresie od 100% do 90% poziom sygnału wyjściowego zmienia się w niewielkim stopniu, jednakże poniżej tej wartości charakter zależności staje się bardziej liniowy.

5.2.6 Eksperymenty na sygnałach rzeczywistych

Pierwsza ocena prototypu, pod kątem zdolności detekcyjnych w warunkach zbliżonych do rzeczywistych, odniesiona została do propozycji określania cechy charakterystycznej, jaką jest czas trwania przerwy w transmisji FHSS pomiędzy sąsiednimi ramkami radiowymi [34]. Na wstępnym etapie nie opracowano jeszcze własnej metody wykrywania dronów, a ten test osiągalny był dla prezentowanego prototypu bez dodatkowych prac implementacyjnych po stronie sprzętowej. Badania przeprowadzone zostały przy użyciu kontrolera Duplex 2,4EX jako źródła sygnału, które było odpowiednikiem tego zastoso-



Rysunek 5.14: Pomiary laboratoryjne toru nadawczego LimeSDR-USB: (a) moc sygnału wyjściowego dla pojedynczego tonu w pełnym zakresie przestrajania, (b) zależność mocy wyjściowej od poziomu wysterowania dla pożądaných częstotliwości zakłócania.

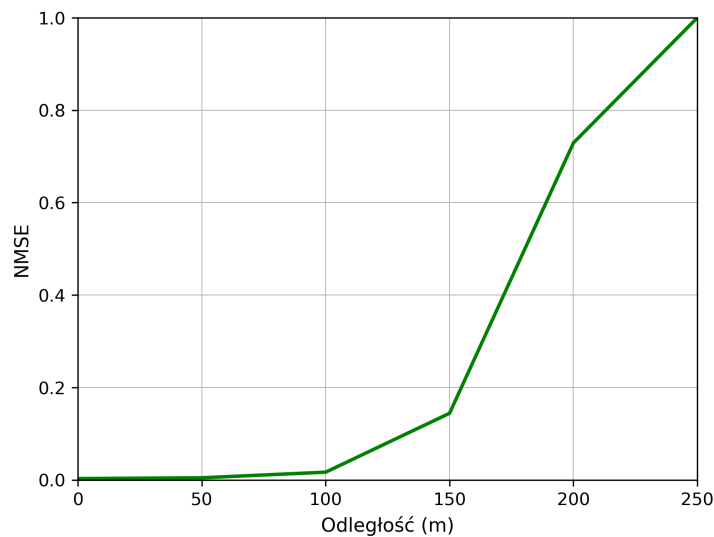
wanego w przytoczonej pracy. Konfiguracja eksperymentalna opierała się na gotowych komponentach, w tym antenie dookólnej, filtry pasmowo-przepustowym do usuwania zakłóceń poza pasmem i Raspberry Pi 4.0. Analiza czasu trwania przerwy między ramkami odbywała się już po STFT, a jakość porównania wartości zmierzonej z rzeczywistą prezentowana była przy pomocy znormalizowanego błędu średniokwadratowego (ang. *Normalized Mean Square Error*, NMSE). Zależność ta może być zapisana jako:

$$NMSE = \frac{1}{N} \sum_{i=1}^N \left(\frac{\hat{t}_i - t}{t} \right)^2, \quad (5.5)$$

gdzie $\hat{t}_i$ jest zmierzonym czasem trwania przerwy, t wartością rzeczywistą, a za N przyjęto wartość 22 zgodnie ze źródłową publikacją. Chociaż charakter zmienności błędu w powiązaniu z odległością w obydwu eksperymentach jest podobny, wyników nie można odnieść do siebie w sposób jednoznaczny z uwagi na brak informacji o parametrach analogowych toru radiowego w cytowanej pracy. Przyjmując jednak zasadność zastosowania proponowanej metody, to za pomocą badanego prototypu osiągnięto wysoką skuteczność detekcji na odległości do 150 m w środowisku zbliżonym do rzeczywistego, co obrazuje rysunek 5.15.

5.3 Przestrajanie szerokopasmowe

Obserwacja widma w czasie rzeczywistym poprzez platformy SDR jest możliwa dla urządzeń z półki w zakresie nieprzekraczającym prędkości przesyłu danych zastosowanego interfejsu i szerokości pasma natychmiastowego końcówki analogowej. Skanowanie szerokopasmowe nie jest domyślną funkcją wykonywaną przez żadne z wymienionych wcześniej urządzeń, a zatem jego efektywna implementacja wymaga dodatkowej pracy. Dwie pod-

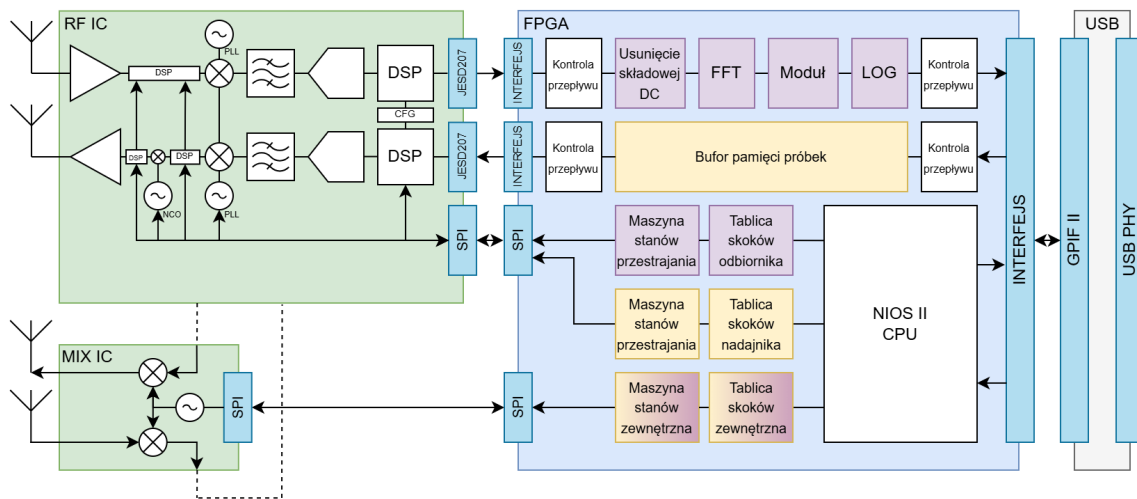


Rysunek 5.15: Znormalizowany błąd średniokwadratowy pomiaru przerwy w transmisji FHSS zrealizowany w warunkach zbliżonych do rzeczywistych.

stawowe formy operacji przyrządów laboratoryjnych stosowanych do szerokopasmowego obrazowania widma to tryb przemiatania oraz tryb FFT. W podejściu klasycznym stosuje się filtr o przestrajanej częstotliwości środkowej i detektor do określania poziomu sygnału w zakresie przenoszenia filtra. Okres przemiatania to czas potrzebny do przeskanowania przez urządzenie danego zakresu częstotliwości. Analizatory widma oparte na FFT natomiast wykorzystują bardzo szybkie przetworniki analogowo-cyfrowe i w sposób programowy przekształcają przebieg z dziedziny czasu do dziedziny częstotliwości. Szerokość pasma chwilowego określa zakres pracy analizatora w tym trybie, a okres przemiatania definiuje czas pomiędzy dwoma kolejnymi rezultatami FFT.

Łącząc oba sposoby, można obserwować szerokie widmo jako złożenie wielu sąsiednich wyników transformacji czasowo-częstotliwościowej określonej na różnych częstotliwościach środkowych w technice o nazwie FFT z przemiataniem (ang. *swept FFT*). W tym procesie następuje akwizycja określonego zestawu próbek podczas przebywania na każdej częstotliwości środkowej, a po wykonaniu transformacji uzyskiwany jest fragment obrazu widma. Zazwyczaj kolejne zakresy skanowania nakładają się na siebie w około 10% w celu wyeliminowania efektu zwiłania wprowadzanego przez filtr pasmowy (ang. *filter roll-off*) na krawędziach obserwowanego pasma. Odstęp pomiędzy kolejnymi fazami próbkowania, niezbędny do przestrojenia parametrów, nazywany jest czasem ślepy (ang. *blind time*).

Aby urządzenie SDR mogło działać jako szerokopasmowy analizator widma ponad swoim pasmem natychmiastowym, konieczne jest wielokrotne strojenie parametrów końcówki analogowej podczas przemiatania zadanego zakresu. Proces szybkiej zmiany tych parametrów wiąże się z kilkoma problemami związanymi z odmiennym podstawowym przeznaczeniem tych urządzeń oraz ograniczeniami w oprogramowaniu, które mają wpływ na końcową prędkość przemiatania. Pierwszą kwestią jest czas potrzebny na wysłanie zestawu



Rysunek 5.16: Schemat blokowy prototypu SDR ze zwiększonym udziałem FPGA w procesie detekcji i przeciwdziałania komercyjnym bezzałogowym statkom powietrznym.

poleceń konfiguracyjnych z aplikacji użytkownika przez interfejs do kontrolera wewnątrz FPGA, a następnie przetworzenie go i w sposób szeregowy dostarczenie do końcówki analogowej. Drugim czynnikiem jest czas strojenia PLL, który zależy od wersji sprzętowej urządzenia, żądanych ustawień i odległości kolejnego skoku częstotliwości. Dodatkowo, proces automatycznej korekcji niedoskonałości toru analogowego wymaga pewnego czasu na ustabilizowanie się natychmiast po dostrojeniu. Powoduje to, na przykład, znaczące błędy składowej stałej w początkowej partii pozyskanych próbek IQ, co może być powodem nieuwzględnienia ich w kalkulacjach FFT. Opisane w tej sekcji modyfikacje związane z przestrajaniem są przedmiotem drugiej autorskiej publikacji [16]. Finalna architektura prototypu opisana w tym rozdziale pokazana jest na schemacie 5.16. W przestrzeni FPGA kolorem fioletowym oznaczone są bloki odpowiedzialne za zmiany w torze odbiorczym, a kolorem żółtym w torze nadawczym. Dodatkowo wyróżniono gradientem ścieżkę do kontroli dwukierunkowej zewnętrznego układu przemiany częstotliwości.

5.3.1 Analiza dostępnych rozwiązań

Przykładowym narzędziem do szerokopasmowej analizy widmowej w kategorii przyrządów do tego przeznaczonych może być RSA503A firmy Tektronix. To niewielkie urządzenie zasilane bateryjnie, które pokrywa zakres częstotliwości od 9 kHz do 3 GHz, charakteryzuje się natychmiastowym pasmem 40 MHz, a prędkość przemiatania określana jest jako 70 GHz na sekundę. Urządzenie łączy się z aplikacją użytkownika poprzez USB, tworząc wszechstronny analizator widma z zaawansowanymi funkcjami pomiarowymi. Dzięki wyeliminowaniu wbudowanego wyświetlacza możliwa jest eliminacja ograniczeń poprzednich przenośnych konstrukcji, w których ścieżka przetwarzania sygnału była dostosowana do możliwości odświeżania ekranu. W tym przypadku restrykcje związane z limitem trans-

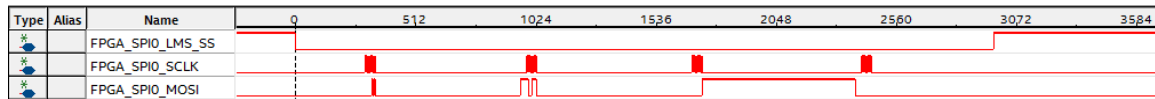
feru USB 3.0 są tożsame dla SDR, jak i dla omawianego urządzenia. Mimo iż jest to tylko podstawowa wersja analizatora, SDR wybrany do obecnego projektu jest niemal dziesięciokrotnie tańszy.

Czysto programowe rozwiązanie szerokopasmowej analizy widma oparte na USRP-B210 i dodatkowym module sterującym w GNU Radio zaprezentowane zostało w opracowaniu [165]. W trakcie analizy podkreślono znaczny udział składowej stałej w pierwszej partii próbek IQ z SDR po wykonaniu skoku częstotliwości środkowej, co wymusiło pominięcie początkowego fragmentu danych. Finalnie, tym sposobem pasmo 100 MHz zobrazowane zostało w 0,875 sekundy, a więc prędkość przemiatania wyniosła 87,5 MHz na sekundę. Rozwiązanie problemu opóźnienia w przypadku sterowania procesem z komputera PC oraz minimalizacja czasu ślepego poprzez przeniesienie kontroli przemiatania do oprogramowania SDR pozwoliła na osiągnięcie szybkości skanowania na poziomie 8 GHz na sekundę [166]. Autorzy pominieli jednak dalsze analizy związane z kalibracją toru i zdecydowali się na stałe pominięcie próbek z pierwszych 820 μ s po każdym ponownym dostrojeniu, aby pozwolić na ustabilizowanie się końcówki analogowej. Poza tym, mimo że obliczenia FFT są zaimplementowane programowo na SDR, sygnał ponownie transformowany jest do dziedziny czasu po złożeniu obrazu widma z fragmentów, aby zachować kompatybilność z dotychczasową aplikacją użytkownika, co jest podstawowym ograniczeniem tego podejścia. Wybrany przez autorów w tym projekcie SDR nie posiadał pojemnego FPGA i za wszystkie procesy odpowiadał procesor ogólnego przeznaczenia znajdujący się na płycie SDR.

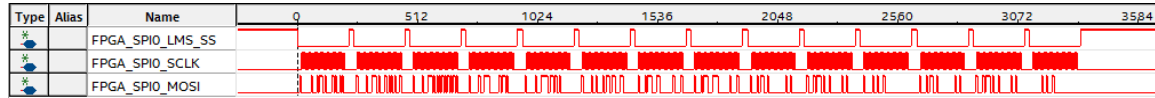
5.3.2 Implementacja metody w torze odbiorczym

W oprogramowaniu dostarczonym przez producentów analizowanych układów SDR konfiguracja PLL wyznaczająca częstotliwość środkową wysyłana jest poprzez USB z aplikacji użytkownika, przez procesor wbudowany wewnątrz FPGA, do końcówki analogowej interfejsem SPI. Przeniesienie mechanizmu sekwencyjnego strojenia do FPGA jest kluczowym czynnikiem zwiększającym możliwość szybkiego przemiatania widma. Aby wykonać operację przestrajania dla LimeSDR-USB, niezbędne jest ustawienie zestawu sześciu 16-bitowych rejestrów za pomocą synchronicznego interfejsu szeregowego. Aby zbadać ten proces w oryginalnym oprogramowaniu, wykorzystano analizator logiczny SignalTap II, który jest narzędziem wbudowanym w środowisko Quartus II, pozwalającym na obserwację sygnałów wewnątrz struktury programowalnej. Porównanie oryginalnego i zoptymalizowanego procesu transmisji zestawu parametrów SPI przedstawia rysunek 5.17. Można zauważyć, że czas pojedynczej transakcji SPI przy użyciu oryginalnego projektu jest porównywalny z pełną sekwencją kontrolowanych sprzętowo transferów po modyfikacji.

W oryginalnym oprogramowaniu pojedyncza 32-bitowa transakcja SPI wymagana do ustawienia jednego rejestru konfiguracyjnego PLL jest podzielona na cztery 8-bitowe frag-



(a) przebieg oryginalny



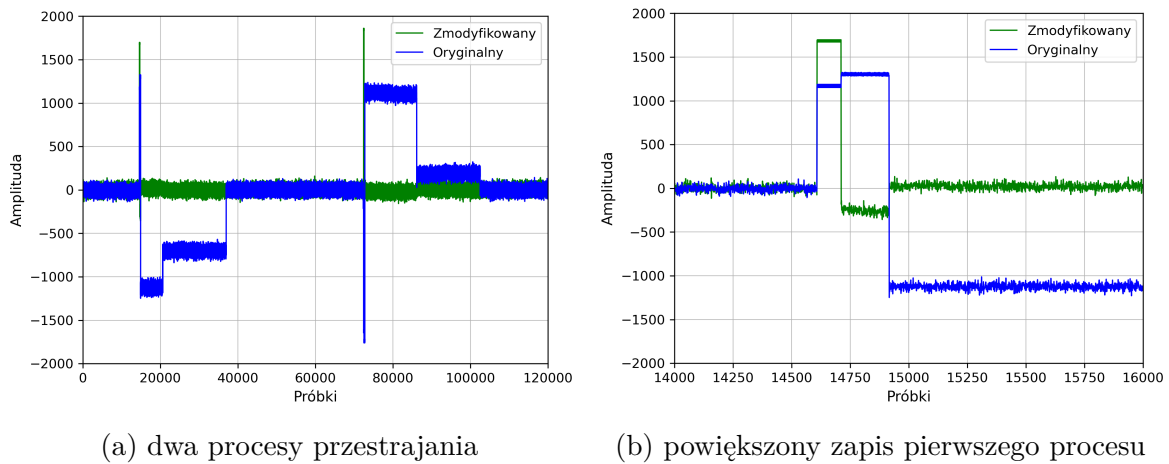
(b) przebieg zmodyfikowany

Rysunek 5.17: Zapis procesu rekonfiguracji PLL w tej samej skali dla oryginalnego oprogramowania i pojedynczej wartości rejestru oraz zmodyfikowanego oprogramowania i pełnego zestawu rejestrów.

menty. Co więcej, ze względu na opóźnienie poleceń wysyłanych po USB, odstęp czasowy między kolejnymi 32-bitowymi transmisjami SPI wynosi ponad kilkadziesiąt mikrosekund. Przeprojektowany moduł SPI może przeprowadzić pełen cykl transakcji odczytu i zapisu w trybie seryjnym, wymaganych do wykonania rekonfiguracji. Dodatkowo, niwelując opóźnienia zapytań generowane przez interfejs USB, możliwa jest zmiana stałego opóźnienia na mechanizm dynamicznego określania momentu zatrzaśnięcia PLL. Po ustawieniu zestawu parametrów rejestr statusowy PLL jest stale odczytywany, więc czas najgorszego opóźnienia nie musi być określony z góry.

Proces automatycznej korekcji niedoskonałości toru analogowego jest kolejnym elementem wpływającym na finalną prędkość szerokopasmowego obrazowania widma. Najważniejszy jego składnik stanowi eliminacja składowej stałej w torze IQ za pomocą pętli kompensacji, która w czasie rzeczywistym wykorzystywana jest do śledzenia i korekcji wszelkich zmian w torze odbiorczym spowodowanych fluktuacjami poziomu sygnału lub efektami temperaturowymi. Jest to korekcja analogowa, która polega na kontrolowaniu prądu polaryzacji wejściowego wzmacniacza sygnału radiowego. Proces ten jest również ważny dla zapewnienia pełnego zakresu dynamicznego przetwornika analogowo-cyfrowego i zapobiegania nasyceniu.

Jedyny programowalny parametr w tej pętli kalibracji to długość okna uśredniania, jednakże nie istnieje mechanizm synchronizacji czy wymuszania chwili, w którym dane mają rozpocząć wypełnianie okna. Niemożliwe jest więc zapełnienie bufora próbkami dokładnie od momentu przestrojenia nowej częstotliwości, ale wartości wypracowane w tym procesie można odczytać i zapisać. Dostęp do nich jest jednak utrudniony i wyzwalany zmianą określonego bitu w ramce SPI, co implikuje sekwencję kilku transakcji niezależnie dla komponentów I i Q. Jeśli ta procedura sterowana byłaby z aplikacji użytkownika, to kilkukrotna dwustronna wymiana danych poprzez interfejs USB trwałaby dłużej niż okno automatycznej korekcji. Reakcja końcówki analogowej na szybkie przełączenie na nową częstotliwość została przedstawiona na wykresie 5.18a. Cykliczny charakter akwizycji danych w oknie wyliczania wartości kalibracyjnych sprawia, że poprawna odpowiedź



Rysunek 5.18: Wartości próbek po zmianie częstotliwości środkowej odbiornika obrazujące proces korekcji składowej stałej w oryginalnym i zmodyfikowanym oprogramowaniu.

korektora jest wypracowywana w dwóch krokach. Gdy przestrojenie nastąpi w okolicach środka trwania okna, wiele próbek pobranych przed lub nawet w trakcie procesu ma wpływ na wyliczone parametry i korekcja jest niepełna. Podczas oczekiwania na automatyczny korektor następuje degradacja zakresu dopuszczalnego sygnału wejściowego, może dojść do nasycenia ADC i zniekształcenia pomiaru. W zmodyfikowanym podejściu, dla przedstawionego przykładu, wystarczy około 350 próbek aby dane nadawały się do dalszego wykorzystania, a w wersji oryginalnej odrzucone zostaje ich nawet 22000 5.18b.

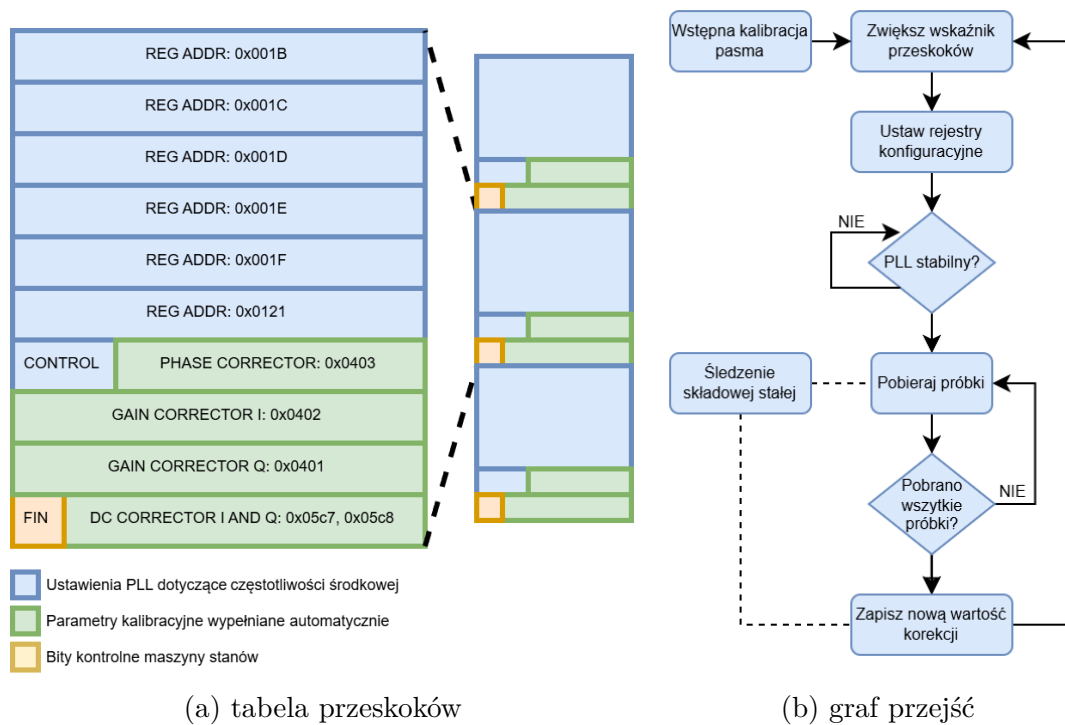
Podczas wstępnych eksperymentów zaobserwowano krótkoterminową powtarzalność wartości korektora związanych z określoną częstotliwością środkową. Dzięki temu korektor może działać w tle, a obliczone rejestry po każdym etapie akwizycji próbek mogą być odczytane, przechowane w pamięci podręcznej FPGA i przywracane podczas powrotu do tej samej częstotliwości środkowej w kolejnym cyklu. Rozwiązanie to umożliwia pominięcie znacznie mniejszej liczby próbek początkowych. Oprócz tej korekcji analogowej, każda ścieżka sygnału posiada matematyczny korektor składowej stałej wypracowany dla każdego okna obserwacji przed FFT. Połączenie korekcji analogowej i cyfrowej kompensuje fakt używania w pierwszym kroku po przestrojeniu parametrów z innej chwili czasu. Opóźnienie interfejsu pomiędzy aplikacją sterującą a końcówką analogową jest na tyle duże, że procedura ta nie ma zastosowania w oryginalnym oprogramowaniu. Będzie ona również nieopłacalna bez jednoczesnej akceleracji wymiany danych po samym SPI. Co więcej, ponieważ korektor i źródło próbek IQ mają niezależne interfejsy dostępu, czynność ta może być wykonywana w tle dzięki możliwości pracy równoległej komponentów FPGA.

Przesunięcie fazowe i niedopasowanie wzmocnienia między składowymi I i Q, w przeciwieństwie do składowej stałej, nie mogą być śledzone i automatycznie eliminowane w tle. Dostrajanie tych parametrów jest procesem iteracyjnym, wymagającym wewnętrznego sygnału wzorcowego. Podczas budowania demodulatora dla zaawansowanego schematu

modulacji, kalibracja tych wartości stanowi istotny aspekt. Nie należy jej także zaniedbywać przy budowie analizatora widma, ale jest ona mniej istotna niż kalibracja składowej stałej. Z tego powodu etap kalibracji tych parametrów przebiega raz w pierwszym kroku procedury przemiatania zdefiniowanego pasma, lub może być wywołany w założonym odstępie czasu. Po zakończeniu operacji wstępnego przemiatania, dane kalibracyjne są przechowywane w sekcji pamięci podręcznej FPGA powiązanej z odpowiednią częstotliwością środkową.

Wybrany schemat przemiatania w zbudowanym prototypie nie musi być z góry zdefiniowany i można go zapisać w formie tabeli przeskoków, która przechowywana jest w pamięci wewnętrznej FPGA. Jedna komórka tabeli, określająca zakres danej częstotliwości środkowej, składa się z dziesięciu 16-bitowych pól, a maszyna stanów kontrolera przemiatania sterowana jest jej zawartością. Pierwsze sześć pól w komórce definiuje parametry PLL niezbędne do ustawienia częstotliwości środkowej. Korektor fazy wymaga jedynie 12 z 16 dostępnych bitów, więc pozostała część siódmego rejestru przeznaczona może być na dodatkowe pola konfiguracyjne, określające ilość powtórzeń skanu na aktualnej częstotliwości. Ta metoda umożliwia bardziej kontrolowane przemiatanie, gdy na pewnych częstotliwościach należy skupić się bardziej, lub szybkie skanowanie całego pasma, gdy wartość na tej pozycji jest ustawiona na zero. Korektor składowej stałej, znajdujący się na ostatniej pozycji w komórce, wymaga tylko 14 bitów, więc pozostałe 2 bity są używane do określenia, czy maszyna stanów powinna powrócić do początku tabeli przeskoków i uruchomić ponownie proces. Mapę komórki dla pojedynczego przeskoku opisuje schemat 5.19a. Metoda ta zapewnia pełną kontrolę nad procesem skanowania jedynie poprzez wypełnienie zawartości pamięci wewnętrznej. Przestrzeń ta może być dynamicznie edytowana poprzez aplikacje użytkownika, bez wprowadzania jakichkolwiek zmian w kodzie FPGA. Tak zaprojektowany system pozwala dodatkowo na selektywne przemiatanie widma, więc wzorce skanowania nie muszą być ciągłe. Jest to niemożliwe w modyfikacji przedstawionej w [166], która określa jedynie częstotliwość początkową i końcową, ani w laboratoryjnym analizatorze widma pracującym w ciągłym paśmie. Schemat maszyny stanów kontroli prezentuje graf 5.19b. Dodatkowo, aby zachować poprawność przesyłu danych w warstwie transportowej, zamiast dostarczania surowych danych do aplikacji użytkownika i skorygować potencjalne straty wynikające z potencjalnego przepełnienia buforów USB, wprowadzono określone pakowanie informacji. Struktura ramki oparta jest na preambule, znaczniku pozycji komórki w tabeli przeskoków, miejscu na dane właściwe i dodatkowej sumie kontrolnej.

Finalnie, konfigurując częstotliwość próbkowania na 96 MHz, zakładając 35 μs na ustawienie rejestrów zgodnie z tabelą przeskoków, oraz 350 próbek na korekcję składowej stałej, otrzymujemy czas ślepy wynoszący około 40 μs . Choć prezentowana implementacja w pewnych momentach jest specyficzna dla wybranego modułu SDR, to obserwacje poczynione w kontekście podobnego układu końcówki analogowej w opracowaniu [165] pokazują, że podejście to można przenieść także na inne urządzenia.



Rysunek 5.19: Zasada działania procesu przemiatania częstotliwości sterowanego z wewnętrznej struktury FPGA.

5.3.3 Implementacja metody w torze nadawczym

Tor nadawczy w SDR podlega podobnym ograniczeniom związanym z interfejsem kontrolnym sterowanym przez aplikacje użytkownika, jak ma to miejsce w torze odbiorczym. W rozdziale poprzednim zlikwidowany został dla prezentowanego prototypu wpływ ograniczenia transferu USB na przepływ strumieni IQ zarówno w torze odbiorczym, jak i nadawczym. Dla toru odbiorczego była to między innymi implementacja sprzętowa FFT, a dla nadawczego system odtwarzania strumienia z pamięci wewnętrznej SDR.

Modyfikacje oprogramowania SDR dotyczące przyspieszenia przestrajania końcówki analogowej opisane dla toru odbiorczego mogą być wykorzystane także przy generowaniu sygnałów zakłócających. Ma to szczególne zastosowanie w technice związanej z przemiataniem częstotliwości, gdyż pokrycie zakresu szerszego niż pasmo natychmiastowe końcówki analogowej wymaga przestrojenia PLL. Proces nadawania szerokopasmowego, przy założeniu odtwarzania strumienia IQ z pamięci SDR, jest bardzo podobny do procedury odbiorczej wykorzystującej akcelerację SPI, tabele przemiatania i wewnętrzną maszynę stanów.

Opisana powyżej technika może być zastosowana niezależnie od układu końcówki analogowej. Układ LMS7002M posiada jednak w torze przetwarzania sygnałów specyficzny dla tego rozwiązania mieszacz zespolony, pozwalający na dodatkowe przesunięcie częstotliwości lub fazy po wymnożeniu z sygnałem oscylatora numerycznego (ang. *Numerically Con-*

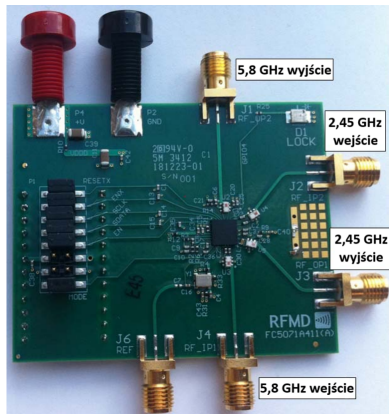
trolled Oscillator, NCO). Cyfrowy sygnał kwadraturowy generowany jest metodą DDFS (ang. *Direct Digital Frequency Synthesis*) z 32-bitowym akumulatorem i 19-bitową precyzją fazy, co pozwala na wytworzenie 14-bitowej fali sinusoidalnej i kosinusoidalnej o niskiej zawartości zniekształceń. NCO jest sterowalny prostymi komendami po SPI, a więc w zakresie generowania przebiegu z modulacją FSK lub PSK może on zostać wykorzystany do bezpośredniego wytwarzania sygnałów zakłócających bez konieczności nawet odtwarzania strumienia IQ z pamięci urządzenia. W tym przypadku wystarczająca do sterowania procesem jest także tożsama z zaimplementowaną wcześniej tabela przeskoków i maszyna stanów wewnątrz FPGA.

5.3.4 Rozszerzenie zakresu częstotliwości

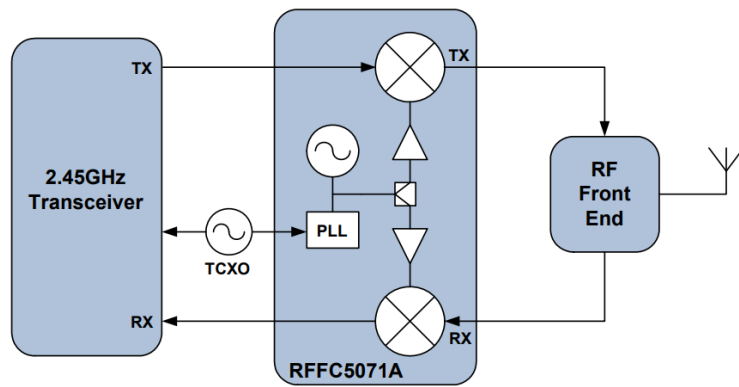
LimeSDR-USB oraz USRP-B210 opierają się na podobnej architekturze składającej się z wysoko zintegrowanej końcówki analogowej. Poza ograniczaniem maksymalnej częstotliwości toru analogowego do 3800 MHz dla LimeSDR-USB, oba urządzenia współdzielą PLL w obrębie każdego kanału, mimo że posiadają dwa kanały nadawcze i dwa odbiorcze. Oznacza to, że dostępność dedykowanego nadawczego PLL i odbiorczego PLL nie pozwala odbierać czy nadawać jednocześnie w dwóch różnych zakresach częstotliwości. Rozwiązaniem tych niedogodności może być zastosowanie dla jednego z torów zewnętrznej przemiany częstotliwości.

RFFC5071A to wysoce zintegrowany układ zawierający dwa miksery, syntezer ułamkowy i oscylatory sterowane napięciem. Miksery są szerokopasmowe i mogą pracować do częstotliwości 6 GHz zarówno dla konwersji w górę, jak i w dół. Wszystkie parametry związane z zarządzaniem układem strojone są po interfejsie SPI, a ich kontrola również odbywać się może bezpośrednio z maszyny stanów w przestrzeni FPGA. RFFC5071A zastosowany został w SDR o nazwie HackRF [167], którego architektura posiada dużo mniejszy stopień integracji w stosunku do opisywanych LimeSDR-USB oraz USRP-B210. Układ przemiennika w tamtej konstrukcji jest niezbędny dla uzyskania możliwości pracy szerokopasmowej, gdyż końcówka analogowa przeznaczona jest wyłącznie do pracy w zakresie od 2,3 GHz do 2,7 GHz. Dodatkowo, zastosowane tam zewnętrzne przetworniki ADC posiadają jedynie 8-bitową rozdzielczość i 20 MHz częstotliwość próbkowania. Brak układu FPGA w tym rozwiązaniu finalnie spowodował, że HackRF nie był rozważany jako platforma do budowy opisywanego prototypu.

Dedykowany zestaw ewaluacyjny dla RFFC5071A przeznaczony dla dwukierunkowej przemiany między pasmem ISM 2,4 GHz a ISM 5,8 GHz, przedstawiony jest na rysunku 5.20a. Płyta scharakteryzowana została dla częstotliwości oscylatora wynoszącej 3350 MHz, co powoduje, że częstotliwość środkowa 5800 MHz widziana przez SDR jest jako 2450 MHz i odwrotnie. Schemat koncepcyjny tego procesu zobrazowany został na rysunku 5.20b. Straty konwersji dla tej konfiguracji częstotliwości i komponentów dla kie-



(a) płyta ewaluacyjna



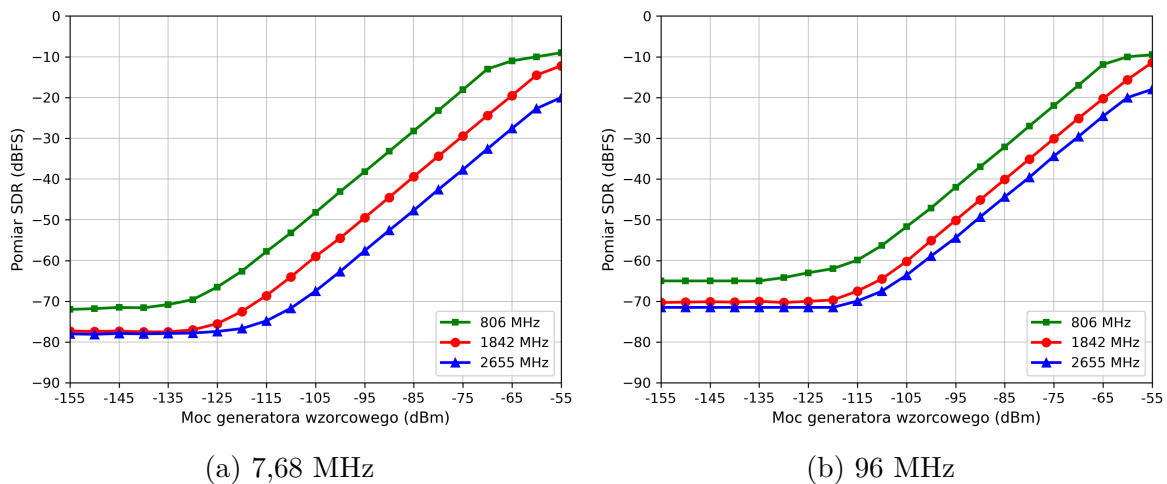
(b) schemat blokowy

Rysunek 5.20: Zewnętrzna przystawka umożliwiająca rozszerzenie zakresu częstotliwości LimeSDR-USB oraz równoległą pracę w dwóch kanałach oparta na RFFC5071A [168].

runku w górę wynoszą 7,0 dB, a dla kierunku w dół na 5,5 dB. W celu wyznaczenia wpływu zewnętrznej przemiany częstotliwości na oba torry określony został dodatkowo współczynnik wektora błędu (ang. *Error Vector Magnitude*, EVM) charakteryzujący w sposób kompleksowy jakość odbiornika lub nadajnika radiowego dla zastosowania w komunikacji cyfrowej. Uwzględnia on różne niedoskonałości związane z szumami czy zniekształceniami toru analogowego, a wyznaczany jest na podstawie przesunięcia rzeczywistych punktów konstelacji w stosunku do tych idealnie rozmieszczonych na diagramie. Podczas pomiarów wykorzystano narzędzia laboratoryjne firmy Rohde&Schwarz, w tym wektorowy generator sygnałów SMJ100A oraz analizator wektorowy FSQ8, a szacunkowy błąd sprzętu testowego został zmierzony na poziomie od 0,4% do 0,5% zarówno przy częstotliwości 2450 MHz, jak i 5800 MHz. Parametr EVM określony przy użyciu sygnału 802.11a/g z modulacją OFDM 64-QAM i przepływnością 54 Mbps wykazał, iż miksery w obu torach nie wprowadzają degradacji większej niż 1% dla mocy wejściowych do 0 dBm [168]. Wyniki zawarte w przytoczonym opracowaniu wskazują, że przy zastosowaniu zewnętrznego miksera można zbudować analogowy tor kształtowania sygnałów, podobny do tego użytego w HackRF, zgodny z warunkami pracy przygotowywanego prototypu.

5.3.5 Pomiary laboratoryjne

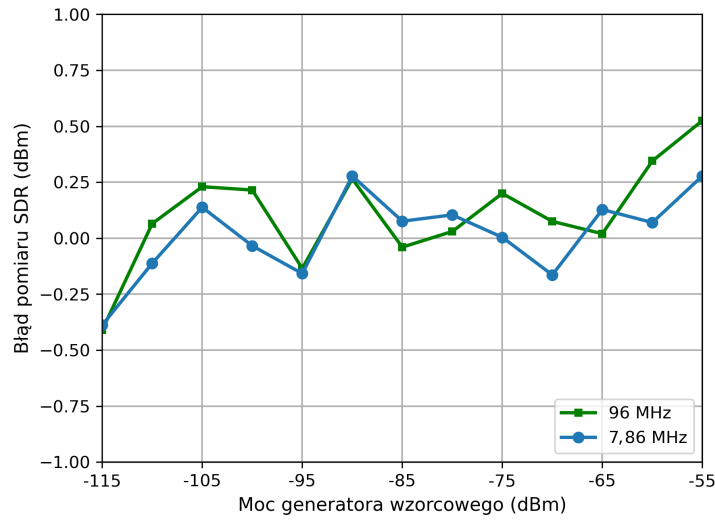
Poziom decybelowy w odniesieniu do pełnej skali określany jako dBFS (ang. *Decibels Relative to Full Scale*) jest naturalnym podejściem do formatowania danych z FFT w implementacji FPGA, ponieważ przeliczenie wartości danego prążka bezpośrednio na moc w dBm wymaga dodatkowej wiedzy o parametrach toru przetwarzania. Aby przełożyć tę wartość na realny poziom sygnału, posłużono się metodą pomiarową, w której zastosowano falę sinusoidalną (ang. *constant wave*, CW) w celu zidentyfikowania liniowego obszaru pracy i poziomu odniesienia dBFS w stosunku do dBm.



Rysunek 5.21: Wyniki pomiarów określające poziom sygnału referencyjnego w dBm odniesiony do dBFS dla różnych częstotliwości środkowych i danej szerokości pasma.

Stanowisko laboratoryjne do kalibrowania odczytu SDR względem cyfrowego generatora Agilent E4432B zestawione zostało przy wykorzystaniu bezpośredniego połączenia kablem koncentrycznym między generatorem odniesienia a urządzeniem badanym. Dla celów analizy wąskopasmowej pomiary wykonano przy szerokości pasma 7,68 MHz z maksymalnym wzmocnieniem analogowym 73 dB, a dla obserwacji silnych sygnałów w obrazowaniu szerokopasmowym zastosowano próbkowanie 96 MHz i wzmocnienie 60 dB. Wszystkie instrumenty zostały włączone dwie godziny przed rozpoczęciem pomiarów, aby osiągnąć równowagę termiczną. Przygotowana konfiguracja pomiarowa zweryfikowana została poprzez podłączenie analizatora Rohde&Schwarz FSV w punkcie wejścia sygnału do SDR, w celu określenia rzeczywistej mocy fali. Częstotliwość sygnału referencyjnego została dobrana eksperymentalnie tak, aby minimalizować rozproszenie między dwoma sąsiednimi prążkami dyskretnymi FFT (ang. *scalloping loss*). Następnie, przy pomocy przygotowanego prototypu sensora zarejestrowano 1000 wektorów FFT o długości 2048 próbek, przestrajając moc fali sinusoidalnej od -155 dBm do -55 dBm w krokach co 5 dBm. Moc sygnału z każdej próby została wyznaczona za pomocą metody MLE ze zbioru pomiarowego, a badania powtórzono dla kilku częstotliwości środkowych. Wyniki pomiarów zaprezentowane są na rysunku 5.21.

Na wykresach można zaobserwować odcinek liniowej zależności między mocą generatora sygnału a wskazaniem opracowanego sensora, jednakże przy różnych częstotliwościach urządzenie daje odmienne odczyty dla tej samej mocy wejściowej. Jest to związane ze znacznym spadkiem wzmocnienia LNA wraz ze wzrostem częstotliwości, gdzie przykładowa różnica pomiędzy punktami 1,0 GHz i 2,0 GHz osiąga 10 dB, a dla 2,0 GHz i 2,5 GHz wynosi 2,5 dB. Dodatkowo, straty wtrąceniowe przełącznika analogowego i transformatora dopasowującego powodują kolejny wzrost tłumienia, które zwiększa się wraz ze wzrostem częstotliwości. Współczynniki kalibracyjne muszą być wyznaczone więc niezależnie dla



Rysunek 5.22: Różnica między mocą wejściową generatora sygnału a odczytem z przygotowanego sensora po kalibracji.

każdej częstotliwości środkowej, aby uzyskać dokładniejsze wyniki finalnych pomiarów. Rezultat zastosowanej procedury kalibracji na odczyty mocy sygnału sinusoidalnego przedstawia wykres 5.22. Za kryterium oceny jakości pomiaru wybrano średni błąd bezwzględny (ang. *Mean Absolute Error*, MAE), który jest zdefiniowany jako 5.6:

$$MAE = \frac{1}{N} \sum_{i=1}^N |\hat{t}_i - t|, \quad (5.6)$$

gdzie $\hat{t}_i$ to wartość zmierzona, t jest wartością referencyjną, a N określa długość serii pomiarowej.

5.3.6 Eksperymenty na sygnałach rzeczywistych

Monitorowanie przestrzeni widma radiowego, w których operują najpopularniejsze komercyjne systemy bezzałogowe, wymaga obserwacji pasma o szerokości 83,5 MHz dla zakresu ISM 2,4 GHz oraz 150 MHz dla zakresu ISM 5,8 GHz. W przypadku pierwszym przestrojenie nie jest potrzebne z uwagi na próbkowanie prototypu sensora z częstotliwością 96 MHz, w przypadku drugim natomiast wystarczy wykonać jedno przestrojenie, aby pokryć ten zakres. Osiągnięty minimalny czas ślepy na poziomie 40 μ s, wymagany do przestrojenia częstotliwości, jest dużo krótszy od standardowego okresu powtarzania sygnałów komunikacyjnych w systemach bezzałogowych, wahających się od kilku do kilkunastu milisekund. W cytowanych wcześniej opracowaniach, niezależnie od dziedziny detekcji, często operowano na fragmentach danych o długości 250 ms, co przy zastosowanej akceleracji przemieszczania i trzech pasmach obserwacji daje czas wciąż poniżej jednej sekundy, potrzebny na zbadanie wszystkich podpasm. Zgodnie z tym można założyć, że dla proponowanych metod następuje ciągła obserwacja danego wycinka widma przez okre-

Tabela 5.1: Zakresy aktualnej pracy sieci 4G/LTE w Polsce.

Pasmo	Downlink (MHz)	Uplink (MHz)	Szerokość (MHz)
B1	2110-2170	1920-1980	60
B3	1805-1880	1710-1785	75
B7	2620-2690	2500-2570	70
B8	925-960	880-915	35
B20	791-821	832-862	30

ślony fragment czasu i dodatkowe eksperymenty związane z wpływem przemiatania na skuteczność detekcji nie są wymagane na tym etapie.

Jak zaznaczono w sekcji odnoszącej się do przeglądu rynku, ścieżka rozwoju bezprzewodowej komunikacji dla urządzeń dronowych rozpoczęła się od modyfikacji protokołów z rodziny 802.11. Zachowując na początku zgodność ze standardem, sygnały statków bezzałogowych nie różniły się od zwykłej wymiany danych w systemach Wi-Fi. Wnioskowanie o obecności drona w zasięgu mogło odbywać się jednak po obserwacji parametrów statystycznych [111][112] lub na podstawie nagłego wzrostu zagęszczenia ruchu sieciowego w monitorowanej przestrzeni [31]. W 2024 roku firma DJI wprowadziła do komercyjnego użytku przystawkę umożliwiającą komunikację niektórych modeli z wykorzystaniem sieci telefonii czwartej generacji, w tym LTE (ang. *Long Term Evolution*), co zrodziło kolejne zagrożenie i otworzyło nową przestrzeń do nadużyć.

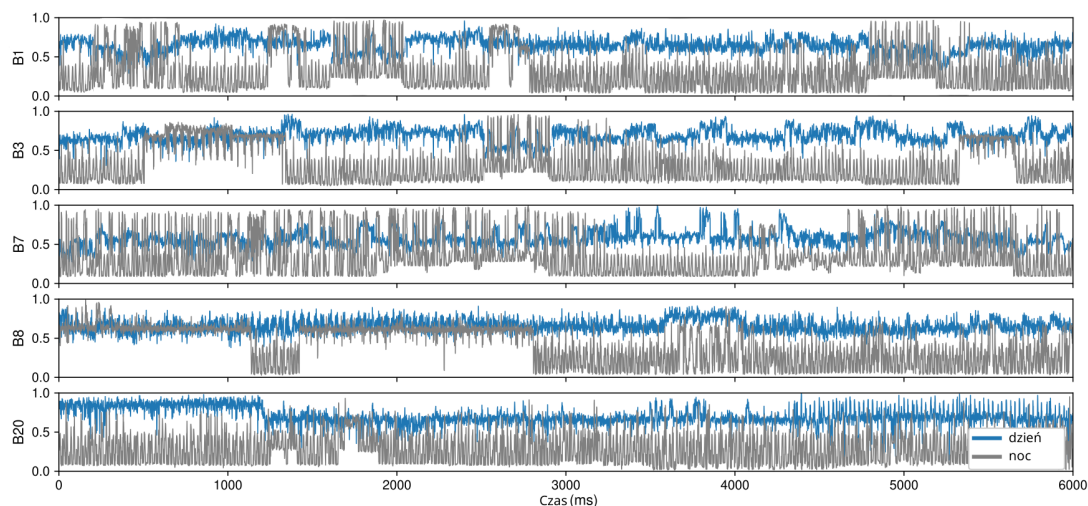
Sieć 4G/LTE zajmuje globalnie częstotliwości w zakresie od 700 MHz do 3600 MHz, a w Polsce operatorzy korzystają z pasm B1, B3, B7, B8 i B20. Dodatkowo większość z podpasm podzielona jest w częstotliwości na 'uplink' i 'downlink', a zastosowania te również charakteryzują się odmiennym typem modulacji. Szczegółowy podział pasm prezentuje tabela 5.1. Proponowany sensor bardzo dobrze nadaje się do analizy tego typu transmisji ze względu na odpowiednią szerokość pasma natychmiastowego, pozwalającą na monitorowanie każdego z zakresów bez konieczności ponownego strojenia i możliwość wykonywania skoków bez potrzeby zachowania ciągłości.

Pewnym pomysłem na wykrycie wtargnięcia drona z modemem LTE może być długotrwałe monitorowanie natężenia ruchu sieciowego, szczególnie w pasmach 'uplinku', gdyż strumieniowanie obrazu na żywo powinno alokować dość duże zasoby. Średni poziom mocy zarejestrowany w poszczególnych kanałach jest odpowiednim wskaźnikiem pozwalającym na zilustrowanie wykorzystania łącza, ponieważ protokół LTE przydziela energię do nośnych tylko wtedy, gdy wysyłane są pakiety. Dodatkowo można niezależnie obserwować podpasmo każdego z operatorów, gdyż posiadają oni indywidualnie wydzielony fragment. Metoda ta posiada pewne ograniczenia związane z prawdopodobnym dużym zagęszczeniem urządzeń w terenach zurbanizowanych, aczkolwiek istnieją pewne scenariusze, w których w połączeniu z innymi technikami jej wykorzystanie może dodać dodatkową wartość. Trudność rozróżnienia transmisji z telefonu komórkowego od tej nadawanej z drona jest także

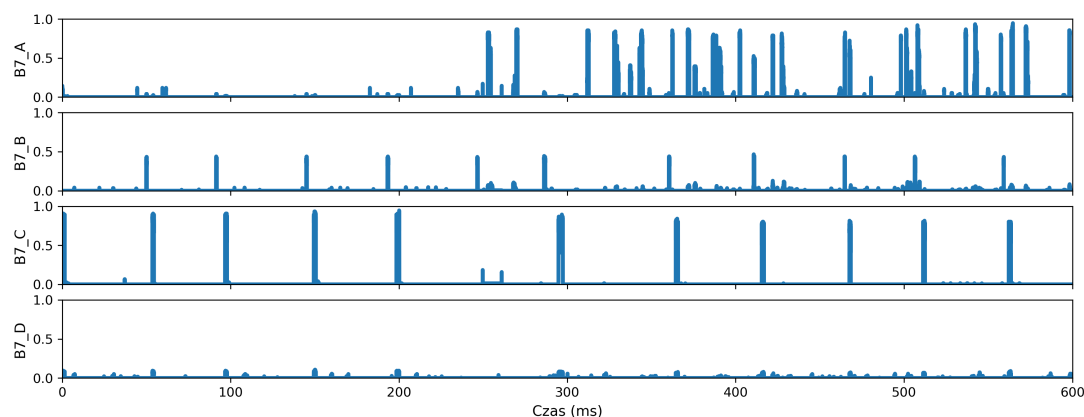
oczywistą wadą tej techniki, choć w przypadku ochrony obiektów infrastruktury krytycznej położonych w mniej zaludnionych terenach, pojawienie się nagłego ruchu w spektrum radiowym, niezależnie od źródła, także może być alarmującym sygnałem.

W opisywanym eksperymencie, wielozakresowa dookólna antena LTE została podłączona do prototypu sensora i zainstalowana w oknie na czwartym piętrze budynku mieszkalnego w wysoce zurbanizowanym obszarze. Czujnik został skonfigurowany do pracy z pasmem 96 MHz ze wzmocnieniem 50 dB, a tabela przeskoków ustawiona do obrazowania wszystkich częstotliwości wymienionych w tabeli 5.1. Aby osiągnąć możliwie największą szybkość przemiatania, w tym przypadku zrezygnowano z priorytetu rozdzielczości częstotliwościowej, toteż dla każdego pasma zbierano 4352 próbki, co pozwala na wykonanie w każdym kanale FFT ośmiu pełnych konwersji o długości 512 punktów z zakładką 50%, a następnie uśrednienie wyniku. Cały cykl pomiarowy, który składał się z 10 etapów akwizycji i przestrojenia, zamykał się w okresie poniżej jednej milisekundy dla wszystkich pasm traktowanych niezależnie. Czas ten jest krótszy niż czas pojedynczej podramki LTE wynoszący 1 ms, więc nie została pominięta żadna transmisja. Aby zoptymalizować proces skanowania, pasma B8 i B20 mogą być agregowane do jednego odczytu, gdyż przerwa częstotliwości między dwoma kierunkami transmisji jest niewielka, lub ograniczyć można liczbę próbek gromadzonych w pojedynczym cyklu.

Prototyp sensora wykorzystany do estymacji zajętości pasma 4G/LTE, może przyczynić się także do późniejszego wnioskowania o występowaniu potencjalnego wtargnięcia systemu bezzałogowego. W eksperymencie tym wykonano szerokopasmową obserwację wszystkich pasm z tabeli 5.1 w trybie przestrajania zgodnie z wcześniejszym opisem. Detekcja poziomu ruchu sieciowego przebiegała niezależnie dla każdej częstotliwości nośnej poprzez progowanie energii w określonej chwili czasu, a następnie znormalizowana była do całości dostępnego dla danego operatora fragmentu widma. Skumulowane wykorzystanie każdego pasma, zbadane w dzień i w nocy, przedstawione jest dla kierunku 'downlink' na wykresie 5.23. Na dzienną zmienność natężenia ruchu sieci komórkowej w tym kierunku wpływają przede wszystkim działania użytkowników internetu. W ciągu dnia średnie wykorzystanie pasm było wysokie i dość stabilne. Zmienia się to znacząco w nocy, kiedy można zaobserwować nagłe skoki energii i nieregularne wzorce. Zróznicowanie w alokacji pasm jest wyraźnie widoczne w różnych porach, jednak należy pamiętać, że obserwujemy tutaj aktywność stacji bazowych, a nie urządzeń końcowych. W kontekście kierunku 'uplink' natomiast, charakter sygnału generowanego przez użytkowników końcowych przedstawiono na wykresie 5.24. Dane zarejestrowane zostały w środku dnia w warunkach podobnych do poprzedniego eksperymentu, a ich prezentacja wykonana jest z dodatkowym podziałem pasma B7 na czterech konkretnych operatorów sieci komórkowych. W pierwszej obserwacji da się zauważyć, iż ogólne wypełnienie pasma jest znacznie mniejsze niż w kierunku przeciwnym. Na przedstawionym wykresie, w okolicy 250 ms, w wydzielonym fragmencie widma B7-A opowiadającym alokacji bieżącego operatora, następuje aktywacja strumie-



Rysunek 5.23: Estymacja ruchu sieciowego 'downlink' w pasmach 4G/LTE w dzień i w nocy w terenie mocno zurbanizowanym.



Rysunek 5.24: Estymacja ruchu sieciowego 'uplink' w paśmie B7 z podziałem na konkretnych operatorów komórkowych. Aktywacja strumieniowania wideo pokazuje zmianę charakteru obciążenia sieci podczas przesyłu dużej ilości danych.

niowania wideo na żywo, co przekłada się na wyraźny wzrost obciążenia i widoczną zmianę jego charakteru. Możliwość wyciągania dalszych wniosków z tych obserwacji odniesiona musi być do charakterystyki konkretnego obiektu chronionego przed wtargnięciem przy modelowaniu możliwych zachowań od strony statku bezzałogowego. W przeprowadzonych eksperymentach udało się wykazać przydatność zmodyfikowanego SDR także w monitorowaniu sygnałów sieci komórkowych, a dalsze prace w tym zakresie pozostawione zostają na etap późniejszy.

Rozdział 6

Badania w dziedzinie detekcji

6.1 Wprowadzenie

Ochrona obiektów infrastruktury krytycznej przed wtargnięciami bezzałogowych statków powietrznych na terenach miejskich stanowi duże wyzwanie, niezależnie od wybranej metody detekcji. Gęsto rozmieszczone zabudowania w tych obszarach niejednokrotnie uniemożliwiają zapewnienie bezpośredniej widoczności pomiędzy obiektem a detektorem. Wykrywanie i śledzenie małych dronów latających na umiarkowanych wysokościach jest więc utrudnione zarówno dla systemów radarowych, jak i rozpoznania optycznego. Dla detekcji akustycznej natomiast problemem w tym obszarze staje się podniesiony szum tła. Rozważając podejście do detekcji na podstawie sygnałów radiowych generowanych przez same drony, także w tym środowisku trzeba polegać na sygnałach odbitych i rozproszonych przez różne przeszkody znajdujące się w otoczeniu.

6.1.1 Modelowanie scenariusza wtargnięcia

Modelowanie środowiska propagacyjnego umożliwia oszacowanie poziomu sygnału w odbiorniku na podstawie parametrów, takich jak częstotliwość, różnica wysokości anten czy charakterystyka otoczenia. Teoretyczne i empiryczne modele propagacji fal radiowych nie są skomplikowane pod względem obliczeniowym oraz w większości przypadków oferują zadowalającą dokładność. Główną ich cechą jest także to, iż sprawdzają się tylko w środowisku podobnym do tego, w którym modele zostały opracowane. W rezultacie modele te na ogół nie dostarczają dokładnych informacji czasowych lub przestrzennych, które są istotne w kontekście planowania rozmieszczenia elementów systemu detekcji radiowej.

Alternatywnym sposobem analizy propagacji jest śledzenie promieni (ang. *Ray Tracing*), które jest narzędziem zapewniającym szacowanie strat mocy fali na ścieżce za pomocą metod numerycznych dedykowanych dla przestrzeni trójwymiarowej. Technika ta może zostać zastosowana dla konkretnego położenia nadajnika i odbiornika w danym obszarze, uwzględniając przy tym geometryczne modele zabudowań, co czyni ją odpowiednią dla

scenariuszy takich jak środowiska miejskie. Wśród promieni generowanych przez źródło punktowe możemy wyróżnić te biegnące bezpośrednio od nadajnika do odbiornika, co jest związane z mechanizmem propagacji w linii wzroku. Jeśli promień natrafi na przeszkodę przed dotarciem do punktu docelowego, symulowany jest proces odbicia i transmisji fali na styku różnych ośrodków. Kierunek dalszej propagacji tego promienia jest zdefiniowany przez prawo odbicia, a jego moc jest określona dla różnych polaryzacji. Wśród wszystkich typów promieni najbardziej skomplikowane jest modelowanie zjawiska dyfrakcji, gdyż jeden promień padający może powodować powstanie wielu promieni rozproszonych. Dodatkowo, obliczenie współczynników dyfrakcji jest znacznie bardziej skomplikowane niż współczynników odbicia czy transmisji, a różne formuły ich wyznaczania mogą dawać odmienne wyniki. W technice tej ogólnie promienie opisywane są jako rury, w których gęstość energii staje się coraz mniejsza w miarę oddziaływania promienia z otoczeniem. Finalnie, całkowite tłumienie ścieżki jest sumą strat interakcji, strat w wolnej przestrzeni i opcjonalnie strat atmosferycznych.

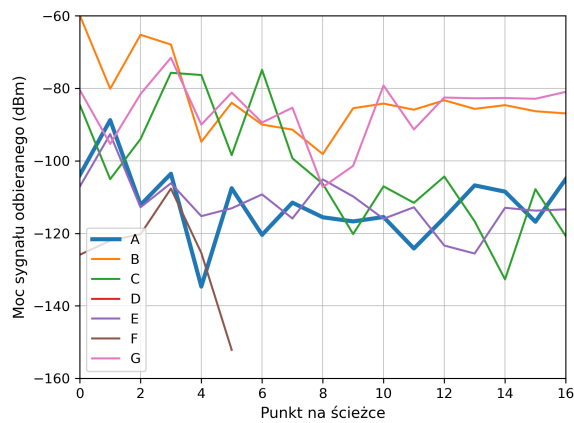
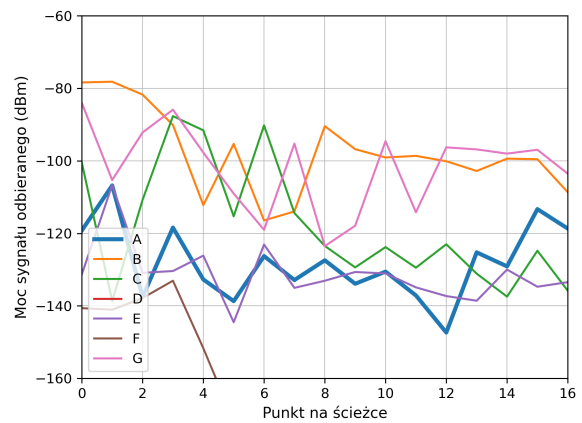
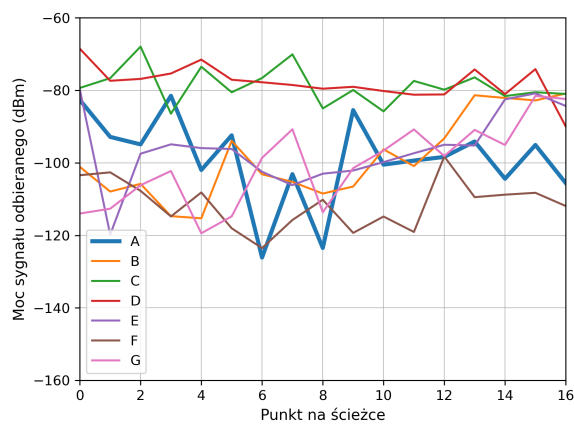
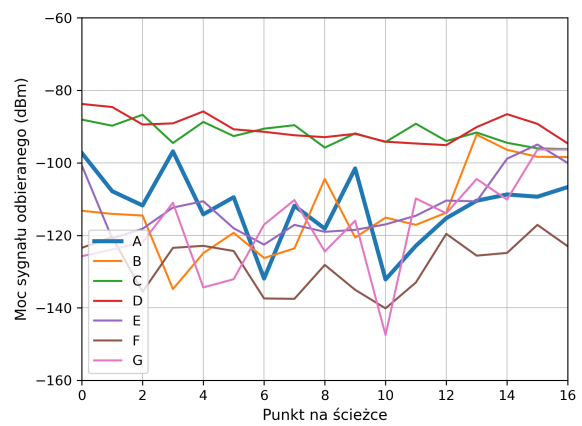
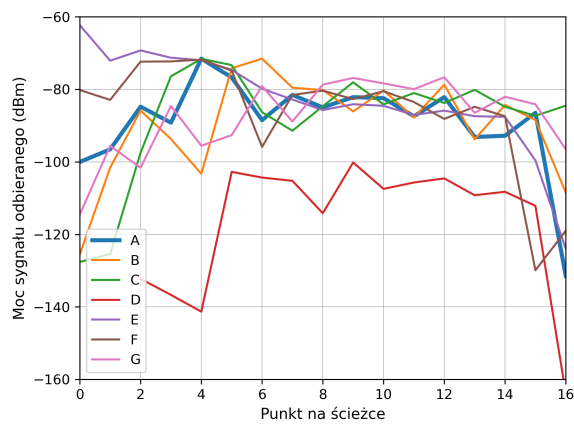
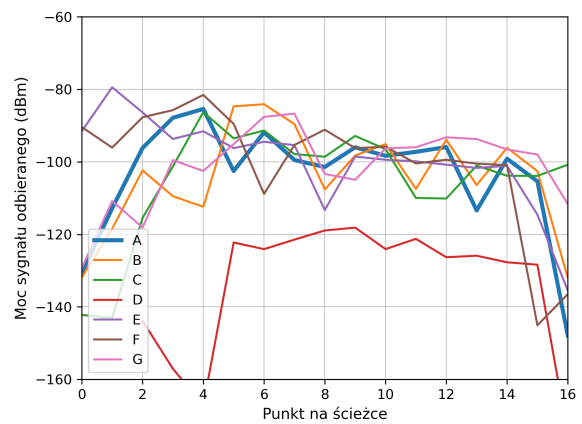
Korzystając z metody analizy promieni, sprzężonej z trójwymiarowym zobrazowaniem terenu, wykonano symulacje mające na celu szacowanie poziomu sygnału w odbiorniku przy wtargnięciu komercyjnego statku bezzałogowego na chroniony teren. Obliczenia wykonane zostały w środowisku Matlab, przy założeniu mocy promieniowania intruza zgodnie ze specyfikacją DJI Mavic 3 wynoszącą odpowiednio 20 dBm dla 2,4 GHz oraz 14 dBm dla 5,8 GHz. Z uwagi na brak wiedzy o antenach stosowanych w konkretnych modelach dronów, przyjęto zarówno dla nadajnika, jak i odbiornika, charakterystykę promieniowania dipola. Modelowym obiektem dla symulacji jest siedziba Zakładów Mechanicznych Bumar Łabędy i Huty Łabędy, znajdująca się w Gliwicach przy ulicy Mechaników. Są to wielkopowierzchniowe obiekty infrastruktury krytycznej, położone w bezpośrednim sąsiedztwie, nastawione na produkcję wojskową.

Podczas eksperymentów zaplanowano trzy możliwe trasy podejścia statku bezzałogowego do rozmieszczonych na obiekcie stacji elektroenergetycznych, które uznane mogą być za elementy krytyczne dla funkcjonowania zakładu. Plan sytuacyjny przedstawiony jest na rysunku 6.1. W symulacji założono możliwości wystąpienia jednego promienia dyfrakcyjnego i dwóch promieni odbitych. Dla propagacji bezpośredniej przyjęto warunki ośrodka gazowego i braku innych wpływów pogodowych, a dla odwzorowania odbić uwzględniono model powierzchni betonowej. Wyniki symulacji poziomu sygnału przedstawiono dla odbiorników umieszczonych na dachach budynków przy założeniu dodatkowej wysokości 3 m, dron pokonywał trasę na wysokości 32 m, a pierwszy i ostatni punkt ścieżki obniżono do 4 m. Analizy przeprowadzono dla czujnika centralnego znajdującego się w punkcie A, oraz dla sześciu czujników rozmieszczonych na budynkach granicznych obiektu w punktach od B do G. Estymacja poziomu sygnału wykonana była w 16 punktach, rozmieszczonych równomiernie po trasie wtargnięcia, gdzie punkt zerowy oznacza położenie modułu stacji elektroenergetycznej. Wyniki eksperymentów przedstawione są na rysunku 6.2. Opisy



Rysunek 6.1: Mapa zakładu Bumar Łabędy z oznaczeniem stacji energoelektrycznych i trasy możliwego wtargnięcia z trzech stron. Punkty niebieskie A – G oznaczają rozmieszczenie sensorów, punkty czerwone natomiast to ścieżka podejścia z wyznaczonymi miejscami wykonania estymacji poziomu sygnału.

w legendach poszczególnych wykresów odpowiadają rozmieszczeniu przedstawionemu na planie sytuacyjnym, a estymacja poziomu sygnału dla stacji centralnej została dodatkowo pogrubiona. W podejściu *I* sensory B i G dostarczają najwyższy poziom sygnału dla obu częstotliwości uwzględnionych w symulacji. W punktach 6 i 4 występuje jednak przesłonięcie ścieżki LOS, co powoduje chwilowe pogorszenie warunków propagacyjnych i lepszy sygnał zanotowano w czujniku C. W podejściu *II* dla całej ścieżki najlepiej wypada sensor D. Dla częstotliwości 5,8 GHz bardzo dobry poziom oferuje także czujnik C, choć dla punktu 3 i częstotliwości 2,4 GHz poziom sygnału większy jest dla detektora A. W scenariuszu *III* natomiast jednoznacznie zidentyfikować można tylko, że najgorszy sensor znajduje się w pozycji D.

(a) *I* - 2,4 GHz(b) *I* - 5,8 GHz(c) *II* - 2,4 GHz(d) *II* - 5,8 GHz(e) *III* - 2,4 GHz(f) *III* - 5,8 GHz

Rysunek 6.2: Wyniki symulacji metodą śledzenia promieni określające poziom sygnału w odbiornikach: (a,b) dla ścieżki *I*, (c,d) dla ścieżki *II*, (e,f) dla ścieżki *III*.

6.1.2 Strategia pracy rozproszonej

Symulacje scenariusza ochrony tego konkretnego obiektu wielkopowierzchniowego przy dość dużej gęstości okolicznej zabudowy pokazują, jak rozmieszczenie przestrzenne czuj-

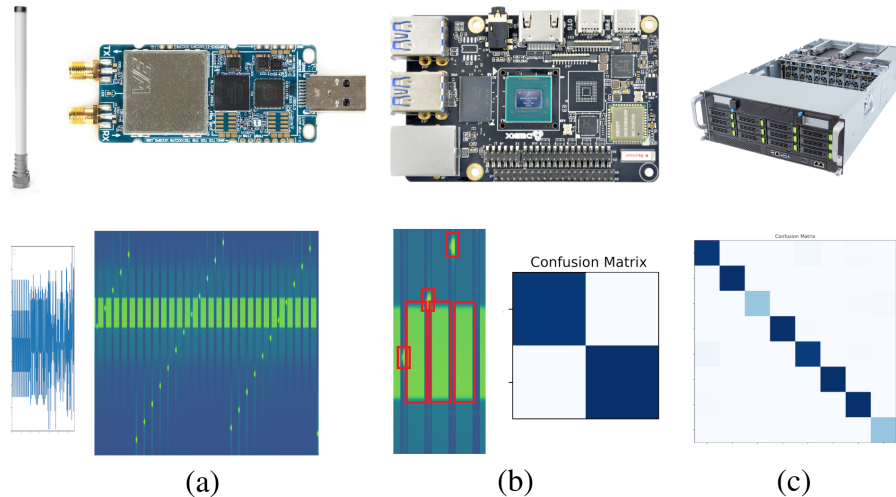


Rysunek 6.3: Koncepcja skalowalnej detekcji rozproszonej dla obiektu wielkopowierzchniowego [18].

ników może zwiększyć poziom pożądanego sygnału w detektorze. W każdym podejściu poziom sygnału przez większość czasu był stosunkowo wysoki dla co najmniej dwóch sensorów, więc wyeliminowano w ten sposób problem pojedynczego punktu awarii, jaki potencjalnie mógłby wystąpić w przypadku samodzielnego detektora centralnego. Dodatkowym atutem tej koncepcji może być także możliwość wyznaczenia punktów wrażliwych i rozmieszczenia w ich okolicy redundantnych czujników, aby jeszcze bardziej podwyższyć poziom prawdopodobieństwa detekcji. Ogólna koncepcja ochrony rozproszonej przedstawiona jest na rysunku 6.3.

Aby ta koncepcja była realizowana, poza minimalizacją kosztu samego sensora, zalecane może być także wykorzystanie istniejącej na obiekcie infrastruktury sieciowej. W przestrzeni przemysłowej nie powinno być problemu z dostępnością sieci LAN (ang. *Local Area Network*) o prędkości 100 Mbps, chociażby z uwagi na obecność monitoringu. Dla przypomnienia jednak, urządzenia, które w sposób natywny zapewniają obserwację surowych danych o pożądanym zakresie widmowym, wymagają interfejsów co najmniej o prędkości 10 Gbps. W związku z tym, mimo osiągniętej na tym etapie akceleracji FFT wewnątrz SDR, wymagane jest także opracowanie algorytmów umożliwiających przeprowadzenie procesu identyfikacji wtargnięcia, możliwych do zrealizowania na sprzęcie o ograniczonej mocy obliczeniowej.

Na schemacie 6.4 zaprezentowano możliwy podział zadań w procesie detekcji komercyjnych bezzałogowych statków powietrznych dla sieci sensorów w koncepcji rozproszonej. W fazie pierwszej, przechwycony sygnał radiowy przechodzi od anteny przez tor kształtowania analogowego i przetwarzany jest do postaci cyfrowej w AFE. Następnie wewnątrz SDR, przy zmodyfikowanym oprogramowaniu, następuje transformacja z dziedziny czasu do dziedziny częstotliwości dla poszerzenia zakresu obserwowanego widma i minimalizacji błędów transferu USB. Gotowy zapis transformaty przekazany jest do lokalnej jednostki obliczeniowej, gdzie na podstawie opracowanych algorytmów następuje podjęcie decyzji



Rysunek 6.4: Łańcuch detekcji w podejściu rozproszonym z podziałem na miejsce wykonywania obliczeń: (a) akwizycja sygnału analogowego i generowanie spektrogramu, (b) detekcja obecności drona i wybór istotnych fragmentów widma, (c) dalsza analiza w centrum fuzji danych.

o obecności drona w zasięgu sensora. W przypadku pozytywnego wykrycia, inicjowany jest transfer zawężonego fragmentu widma do centralnej jednostki fuzji danych w celu dalszej obróbki. Podczas gdy obecność drona w strefie chronionej jest sytuacją wyjątkową, w trakcie normalnego użytkowania obciążenie sieci z uwagi na działanie systemu będzie minimalne, gdyż sygnały sterowania i wideo generowane przez jeden zestaw dronowy wypełniają tylko około 8%-10% przestrzeni widmowej. Wartość ta będzie dodatkowo zminimalizowana, jeśli w fazie detekcji przygotowane i wysłane dalej zostaną tylko te wycinki widma, które zawierają istotne informacje. Aspekt rozwoju funkcjonalności centrum fuzji danych, takich jak klasyfikacja konkretnego modelu drona czy próba określenia lokalizacji na podstawie powiadomień z wielu czujników, zostaje pozostawiony na przyszły etap prac.

Głównym tematem dalszej części rozdziału będzie właśnie analiza algorytmów możliwych do zaimplementowania w jednostce komputera wbudowanego. Ograniczeniem w tym aspekcie jest moc obliczeniowa potrzebna do realizacji zadań w czasie rzeczywistym. Optymalizacja procesu decyzyjnego przeprowadzona będzie na podstawie ogólnodostępnej bazy danych sygnatur radiowych pozyskanej w środowisku laboratoryjnym oraz bazy własnej stworzonej w warunkach zbliżonych do rzeczywistych już przy użyciu opisanego prototypu sensora. Podstawą przedstawionych w tym rozdziale prac jest trzeci artykuł opracowany podczas trwania projektu doktorskiego [18].

6.1.3 Przegląd istniejących baz sygnatur dronowych

Pierwsza ogólnie dostępna baza danych zawierająca zapis radiowych sygnałów pochodzących od komercyjnych bezzałogowych statków powietrznych została zaprezentowana w 2019 roku [169]. Zbiór zawiera nagrania próbek IQ trzech dronów podzielone dodatkowo

na operacje w różnych trybach, takich jak podłączenie, zawis czy lot po trasie, a każde z nich trwa około 5,25 s. Dla uzupełnienia, osobną kategorię stanowią aktywności w tle o długości około 10,25 s, które nie zawierają jasno zdefiniowanych typów działających urządzeń, ale da się w nich zauważyć aktywność sygnałów Wi-Fi. Nagrania podzielone są na fragmenty o długości 250 ms, a rozmiar bazy przekracza 40 GB. Dane pozyskiwane były przy równoległym użyciu dwóch SDR z rodziny USRP, z których każdy pokrywał 40 MHz w paśmie ISM 2,4 GHz. Baza jest często wykorzystywana w badaniach zarówno w aspekcie detekcji binarnej, jak i rozróżniania typów, a nawet trybów pracy urządzeń. Dużym jej minusem jest niska zawartość sygnałów niezwiązanych z systemami bezzałogowymi, bo tylko 18,06%. Dodatkowo, częste straty próbek wynikające z przepełnień w interfejsie pomiędzy SDR a komputerem PC powodują nieciągłości w nagrywanym sygnale, a ich losowy charakter może być mylący dla różnych metod detekcji. Kolejna baza w tej kategorii zawiera nagrania próbek IQ siedmiu modeli dronów pracujących w trybach połączenia, lotu i zawisu [170]. Każde z nagrań powtórzone zostało przy obecności zakłóceń generowanych przez Wi-Fi, Bluetooth oraz oba źródła jednocześnie. Pliki zawierają próbki z około 2 s działania, a rozmiar bazy przekracza 65 GB. Dane pozyskiwane były z pasmem 20 MHz na częstotliwości środkowej 2,4375 GHz, przy użyciu AFE z rodziny LIME poprzedniej generacji w stosunku do tej użytej w opisywanym prototypie sensora. Dużym ograniczeniem tej bazy jest przede wszystkim niepełne obrazowanie pasma ISM 2,4 GHz oraz brak nagrań nie zawierających sygnałów dronowych, które są niezbędne do sprawdzania jakości detekcji binarnej. Dodatkowo, zbiór posiada pewne braki w folderach, co finalnie powoduje, iż nie jest ona często wykorzystywana w eksperymentach.

Wymienione powyżej zbiory tworzone były przy użyciu urządzeń, które w wersji standardowej posiadają opisywane wcześniej ograniczenia pasma i wykazują duże prawdopodobieństwo strat pakietów na interfejsie przy obrazowaniu szerokiego zakresu częstotliwości. W odmiennym podejściu do zbierania danych o sygnałach dronowych można zastosować narzędzia klasy laboratoryjnej, a do akwizycji danych wykorzystać oscyloskop o wysokiej rozdzielczości. W tym przypadku baza nie opiera się na strumieniu IQ, a zawiera przebiegi zmienności amplitudy wykrytego sygnału. Zbiór danych zawierający ponad 1000 nagrań 17 kontrolerów komercyjnych bezzałogowych statków powietrznych, podzielonych na fragmenty o długości 0,25 ms, przedstawiony został w [33]. Zapisany jest przy próbkowaniu 20 GSps na częstotliwości środkowej 2,44 GHz, a rozmiar całości wynosi ponad 124 GB. Początkowo baza zawierała tylko sygnały pochodzące z systemów dronowych, jednakże później została rozwinięta o nagrania Wi-Fi oraz Bluetooth. Z uwagi na bardzo dużą częstotliwość próbkowania, zawarte w niej dane często używane są w metodach detekcji opierających się na opisie parametrów związanych z czasem narostu sygnału radiowego występującym przy początku transmisji ramki. Kolejna interesująca baza z tej kategorii opracowana została przy użyciu laboratoryjnego analizatora widma, który może rejestrować pasmo natychmiastowe o szerokości 110 MHz. Podstawą budowy zbioru są trzy statki

bezzałogowe firmy DJI, których nagrania skatalogowano niezależnie dla czterech trybów pracy oraz aktywności tła. Czas akwizycji każdego sygnału wynosił tutaj 450 ms, nagrania przeprowadzono w obu dostępnych pasmach, a finalny rozmiar bazy to ponad 5,8 GB [171].

W kolejnej kategorii baz danych sygnałów dronowych, podstawę stanowią próbki IQ pozyskane w środowisku laboratoryjnym przez urządzenia SDR USRP X310. W pierwszym zbiorze zawarte są dane z 5 indywidualnych kontrolerów z kategorii modeli RC, a także komunikacja 4 zestawów urządzeń, w skład których wchodził dron i kontroler [172]. Akwizycja sygnałów odbywa się z prędkością 100 MSps na częstotliwości środkowej 2,44 GHz. Każdy plik w bazie zawiera nagranie o długości około 100 ms, co składa się na 50 s nagrań o sumarycznym rozmiarze ponad 43 GB. Baza posiada w większości próbki o wysokiej jakości, jednakże nie wychodzi poza pasmo ISM 2,4 GHz i nie posiada nagrań sygnałów Wi-Fi oraz Bluetooth. Ostatnią analizowaną bazą jest zestawienie nagrań 10 komercyjnych statków bezzałogowych wraz z kontrolerami, pozyskanych w komorze bezodbićowej [173]. Opublikowane dane zostały wybrane w taki sposób, aby w każdym pojedynczym nagraniu uchwycić pełną sekwencję przeskoków sygnału sterującego. Sygnały nagrywane na częstotliwości środkowej 2,44 GHz próbkowane były z prędkością 120 Msps, a czas ich rejestracji wynosił 1 s. Dla częstotliwości środkowej 5,8 GHz prędkość próbkowania osiągnęła 200 Msps, a czas nagrywania to 0,5 s. Całość bazy zawiera 19 plików z danymi mających sumaryczny rozmiar 8 GB. Mimo niewielkich rozmiarów bazy, jest ona bardzo cenna z uwagi na wysoki SNR oraz stały szum tła, pozwalający na prostą dalszą obróbkę sygnału.

6.2 Techniki analizy widma

Analiza widma radiowego przedstawionego w postaci spektrogramu może być traktowana jako pewna forma detekcji obiektów na klasycznych obrazach. Wykrywanie obiektów polega na równoczesnym rozpoznaniu rozmieszczenia i kategorii elementów na danym obrazie. W przypadku poszukiwania ramek radiowych jednak, nie spodziewamy się asymetrycznych kształtów, czy problemów związanych z rotacją i skalowaniem obiektów, a zadanie sprowadza się do wykrywania krawędzi czy zamknięcia spójnego podzbioru pikseli w polu ograniczającym. Kryterium detekcji stać się tu może na przykład gradient intensywności pikseli, pozwalający odróżnić sygnał użyteczny od tła, które w tym przypadku stanowi szum.

Pierwszą badaną metodą jest podejście dwuetapowe, gdzie na początku następuje wykrycie obecności transmisji, a następnie przeprowadzana jest klasyfikacja binarna, określająca przynależność sygnału do systemu bezzałogowego. Etapowy charakter procesu wiąże się z uwzględnieniem podziału zadań i kryteriów jakości dla każdego stopnia. Duża czułość, czyli wykrycie jak największej liczby interesujących elementów w widmie, jest najważniejszą cechą pierwszego etapu, drugi krok natomiast powinien charakteryzować się

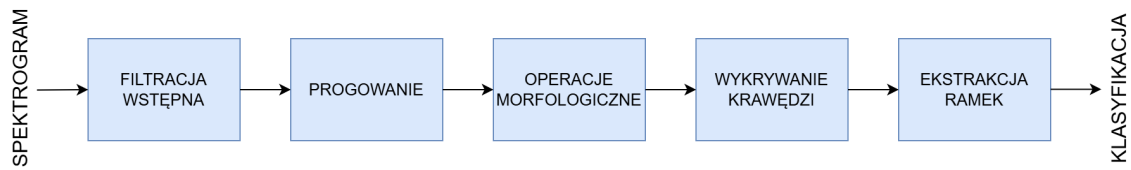
wysoką dokładnością w ich klasyfikacji. Etap pierwszy wykonywany jest za pomocą jednego z klasycznych algorytmów rozróżniających sygnał użyteczny od szumu, co umożliwia jego optymalizację pod kątem złożoności obliczeniowej. Początkowo ten stopień detektora, zaimplementowany był nawet wewnątrz FPGA i SDR, co opisane zostało w przytaczanym już autorskim artykule [15]. Finalnie jednak, dla uzyskania większej uniwersalności prototypu sprzętowego sensora i efektora, ten fragment obliczeń umieszczono w części oprogramowania komputera wbudowanego. Krok drugi natomiast opiera się na algorytmach uczenia maszynowego, gdzie klasyfikowany jest dokładnie przygotowany w poprzedniej fazie wycinek widma. Dzięki temu dobór parametrów w obu procesach może przebiegać niezależnie, a skuteczność rozróżniania sygnałów dronowych od Wi-Fi czy Bluetooth można zbadać dla różnych metod uczenia maszynowego.

W metodzie drugiej eksperymenty dotyczą podejścia jednorodnego, gdzie głęboka sieć neuronowa przejmuje oba zadania, a analizie poddawany jest pełny obraz widma podzielony jedynie na fragmenty w osi czasu. Podejście to powinno optymalizować zarówno czułość detekcji, jak i dokładność klasyfikacji w ramach jednolitego modelu. Detektory obiektów wykorzystujące warstwy konwolucyjne mogą być zrealizowane, w zależności od struktury wewnętrznej, jako jedna lub wiele struktur, razem jednak tworzą one współpracujący zestaw, przetwarzający dane w sposób potokowy. Sprawia to, że całość procesu obliczeniowego jest ulokowana w jednym miejscu i szacowanie złożoności oraz czasu inferencji jest bardziej przewidywalne.

6.2.1 Detekcja klasyczna

W klasycznym podejściu do wykrywania sygnałów wybrana została podstawowa metoda, jaką jest detekcja energii, z uwagi na najprostszy schemat implementacji, także potencjalnie w warstwie sprzętowej, oraz brak konieczności posiadania wiedzy o poszukiwanym sygnale. Wynikiem działania algorytmu na tym etapie jest ekstrakcja ze spektrogramu wycinka widma zawierającego poprawną ramkę radiową, a przygotowany proces pokazany jest na schemacie 6.5.

Zawężając wybór do metody detekcji energii, wciąż można odnaleźć w literaturze wiele propozycji w temacie precyzyjnego obliczenia wartości progowej, która ma kluczowe znaczenie dla skutecznego rozpoznawania sygnałów w widmie. Istotną rolę w osiągnięciu określonej jakości działania całego algorytmu detekcji odgrywa także wyznaczenie odpowiedniej strategii szacowania progu, wśród których wyróżniamy estymacje ze stałą wartością zdefiniowaną z góry oraz metodę adaptacyjną, dostosowującą się w sposób ciągły do zmiennego poziomu szumu. Oba podejścia mają swoje zalety i ograniczenia, a wybór zależy od konkretnej aplikacji. W przedstawionym procesie najważniejszym elementem jest jednak uniwersalność wynikająca z warunków pracy i przestrzennego rozmieszczenia poszczególnych urządzeń, co skutkuje koniecznością poszukiwania metody dynamicznego



Rysunek 6.5: Proces ekstrakcji ramek sygnałów radiowych ze spektrogramu.

obliczania wartości progowej.

Techniki adaptacyjne można głębiej klasyfikować jako lokalne i globalne. Metody lokalne definiują odrębny próg dla każdej próbki w zmierzonym widmie i znane są głównie jako detektory o stałym współczynniku fałszywych alarmów (ang. *Constant False Alarm Rate*, CFAR). Stosowane są one między innymi w kategorii sygnałów radarowych, a ich wady uwiadcniają się przy transmisjach o wysokiej mocy średniej rozłożonej w szerokim zakresie częstotliwości, takich jak modulacje szerokopasmowe. Główną przyczyną tego zjawiska jest efekt pojawienia się składowej stałej i przesunięcia wartości progowej, wynikający z obecności wielu próbek sygnału w oknie obliczeniowym algorytmu [174]. Metody globalne natomiast wyznaczają pojedynczą wartość progową dla całego zakresu próbek w oknie, a do reprezentantów tej kategorii można zaliczyć na przykład metody parametryczne, takie jak ROHT (ang. *Recursive One-sided Hypothesis Testing*) czy FCME (ang. *Forward Consecutive Mean Excision*) oraz rodzinę algorytmów nie wymagających parametrów, opartych na podstawach podejścia Otsu [175].

Algorytm ROHT wykorzystuje metody statystyczne i założenie, że dany zbiór zawiera więcej próbek szumu niż sygnału [176]. Początkowo, uwzględniając parametry takie jak średnia i odchylenie standardowe, wyznaczana jest pierwsza wartość progowa. W każdej iteracji procesu określona liczba próbek w zbiorze większa od progu jest identyfikowana jako sygnały właściwe i odrzucana, a pozostałe są dalej w procesie. Tym samym w każdej iteracji odchylenie standardowe jest stopniowo zmniejszane, aż jego zmiana między kolejnymi krokami stanie się mniejsza od określonej wartości arbitralnej. Algorytm FCME, również należy do metod iteracyjnych, a początkowa wartość progu wyznaczana w nim jest przy założeniu danego współczynnika fałszywych alarmów [177]. Kolejnym predefiniowanym parametrem używanym w obliczeniach jest liczba próbek zawierających tylko składnik szumowy. Zazwyczaj wskazane parametry muszą pozostać niezmiennie, aż do momentu ponownego uruchomienia algorytmu. W pierwszym kroku działania procesu obliczeniowego próbki są porządkowane w kolejności rosnącej zgodnie z ich energią. Następnie wybiera się określony zbiór najmniejszych próbek, aby utworzyć początkowy zestaw zawierający tylko wartości uznawane za szum. W kroku kolejnym obliczana jest wartość średnia powyższego zbioru, która przemnożona przez parametr odniesiony do współczynnika fałszywych alarmów, daje nową wartość progową. Następnie próbki znajdujące się poniżej progu włączane są do zbioru i obliczana jest nowa wartość średnia i próg. Czynność

ta jest powtarzana do momentu, gdy nie będzie nowych próbek poniżej progu. Ostatecznie przyjmuje się, że próbki powyżej progu są próbkami sygnału, a próbki poniżej progu są próbkami szumu. Istnieje bardzo wiele modyfikacji powyższego podstawowego algorytmu. W jednej z metod poleca się rozpoczęcie procesu od wstępnego filtrowania sygnału wejściowego przez filtr medianowy, co znacznie zmniejsza wariancję związaną z szumem i ułatwia dokładniejsze oszacowanie wartości progowych. W innych realizacjach wyższego rzędu natomiast podstawy algorytmu FCME wykorzystywane są przy różnym zestawie parametrów wejściowych do wyznaczenia dwóch wartości progowych.

Powyższe metody, z uwagi na iteracyjny charakter obliczeń, nie sprawdzą się w systemach, gdzie kluczowe jest określenie dokładnego czasu wykonywania danego procesu czy implementacja w zasobach FPGA. Dodatkowo dobór parametrów może być kłopotliwy dla dużej sieci czujników, jeśli wymagane będzie indywidualne strojenie. W poszukiwaniu metody w pełni automatycznej, nie wymagającej procesu iteracyjnego, odwołano się do algorytmu, którego autorem jest Nobuyuki Otsu [69]. Jest to metoda oparta na histogramie, polegająca na maksymalizacji wariancji międzyklasowej, znana z kategorii progowania obrazów, lecz skutecznie może być dostosowana również do analizy widma [178]. Interesujące jej rozwinięcie stanowi także technika NPAQM (ang. *Non-parametric Amplitude Quantization Method*), która nie tylko nie wymaga podania wstępnych parametrów, ale także eliminuje potrzebę generowania histogramu [68]. Alternatywnie, dla określenia optymalnej wartości progowej, podejście to opiera się na różnicy wariancji międzyklasowej pierwszego rzędu, obliczonej na podstawie zbioru posortowanych danych wejściowych. Dodatkowo NPAQM zawiera wbudowany algorytm heurystyczny do identyfikacji przypadków, w których zbiór wejściowy zawiera tylko próbki szumu.

Proces obliczania wartości progowej dla NPAQM rozpoczyna się od posortowania próbek wejściowych pozyskanych z jednego wektora FFT o długości L w kolejności rosnącej tak, aby spełnić warunek $y_{(1)} < y_{(2)} < \dots < y_{(L)}$ i otrzymać zbiór 6.1:

$$Y_l = \{y_1, y_2, \dots, y_L\}. \quad (6.1)$$

Następnie sugerowana jest kwantyzacja zakresu amplitud w celu wybrania najbardziej odpowiedniego kandydata na wartość progową przy jednoczesnym zmniejszeniu złożoności obliczeniowej. Stosując funkcję sufitu $\lceil \cdot \rceil$, poziom kwantyzacji M , określony jest jako 6.2:

$$M = \lceil 1 + \lg_2 L + \lg_2(1 + \frac{|g|}{\sigma_g}) \rceil, \quad (6.2)$$

gdzie funkcja modułu $|\cdot|$ skośności rozkładu g jest wyznaczana jako 6.3:

$$g = \frac{\frac{1}{L} \sum_{i=1}^L (Y_i - \bar{Y}_l)^3}{(\frac{1}{L} \sum_{i=1}^L (Y_i - \bar{Y}_l)^2)^{\frac{3}{2}}}, \quad (6.3)$$

a $\overline{Y}_l$ stanowi średnią zbioru Y_l , gdzie σ_g to 6.4:

$$\sigma_g = \sqrt{\frac{6(L-2)}{(L+1)(L+3)}}. \quad (6.4)$$

W tym momencie krok q , z jakim wykonywane będą obliczenia, można przedstawić wzorem 6.5:

$$q = \lceil \frac{y_{(L)} - y_{(1)}}{M} \rceil, \quad (6.5)$$

gdzie $y_{(L)}$ i $y_{(1)}$ odpowiadają wartościom $\max(Y_l)$ i $\min(Y_l)$, ponieważ próbki zostały wcześniej posortowane. Listę potencjalnych kandydatów na wartość progową można teraz zapisać jako 6.6:

$$Y(m) = \{y_{(1)}, y_{(1)} + q, \dots, y_{(1)} + (M-1)q\}, \quad (6.6)$$

i uprościć zapis do 6.7:

$$\gamma_i = \{\gamma_1, \gamma_2, \dots, \gamma_M\}. \quad (6.7)$$

W kolejnym kroku można już dokonać podziału na dwie grupy. Zbiór $\omega(\gamma_i)$ zawierać będzie tylko próbki szumu, a $S(\gamma_i)$ szumu wraz z sygnałem użytecznym. Zakłada się, że próbki o wartościach poniżej progu to tylko szum, podczas gdy próbki o wyższych wartościach to sygnał plus szum. Przynależność do zbioru $\omega(\gamma_i)$ można wyrazić jako 6.8, a do zbioru $S(\gamma_i)$ jako 6.9:

$$\omega(\gamma_i) = \{Y_{(l)} < \gamma_i\} = \{y_{(1)}, y_{(2)}, \dots, y_{(k)}\}, \quad (6.8)$$

$$S(\gamma_i) = \{Y_{(l)} \geq \gamma_i\} = \{y_{(k+1)}, y_{(k+2)}, \dots, y_{(L)}\}, \quad (6.9)$$

co wyznaczane jest dla wszystkich elementów z (6.7), gdzie k jest liczbą elementów mniejszych od γ_i . Obliczenia wariancji międzyklasowej dla każdego elementu z (6.7) można zapisać jako 6.10:

$$\sigma^2(\gamma_i) = P_s(\gamma_i)P_\omega(\gamma_i)[\overline{S}(\gamma_i) - \overline{\omega}(\gamma_i)]^2, \quad (6.10)$$

gdzie $P_s(\gamma_i)$ jest prawdopodobieństwem dla wystąpienia sygnału i $\overline{S}(\gamma_i)$ jest średnią zbioru 6.9, $P_\omega(\gamma_i)$ jest prawdopodobieństwem wystąpienia elementów szumu, a $\overline{\omega}(\gamma_i)$ jest średnią zbioru 6.8. Prawdopodobieństwa te można natomiast przedstawić jako 6.11:

$$P_s(\gamma_i) = \frac{k}{L}, \quad P_\omega(\gamma_i) = 1 - \frac{k}{L}, \quad (6.11)$$

gdzie k jest liczbą elementów w każdym zbiorze. Finalnie, funkcja różnicy pierwszego rzędu obliczana jest zgodnie z 6.10 w zakresie $m = 1, 2, \dots, M-1$, co zapisane jest jako 6.12:

$$\lambda_m(\gamma_i) = |\sigma_{m+1}^2(\gamma_i) - \sigma_m^2(\gamma_i)|. \quad (6.12)$$

Optymalny próg jest określany przez wartość, która minimalizuje 6.12, co można przedstawić jako 6.13:

$$\lambda(\gamma^{eff}) = \min \lambda(\gamma_i), \text{ dla } \gamma_i = \{\gamma_1, \gamma_2, \dots, \gamma_M\}. \quad (6.13)$$

Uzupełnieniem powyższej metody jest technika heurystyczna wykorzystująca stopień bliskości między obliczonym progiem $\lambda(\gamma^{eff})$, a średnią całkowitego zbioru próbek Y_l , w celu identyfikacji sytuacji, w których w zbiorze wejściowym znajduje się wyłącznie szum. Przypadek ten ma miejsce, jeśli spełnione są warunki 6.14 i 6.15:

$$\lceil \gamma^{eff} \rceil \leq \lceil \mu_Y \rceil, \quad (6.14)$$

$$|\mu_Y - \gamma^{eff}| \leq 10 \times [y_{(F)} - y_{(1)}], \quad (6.15)$$

gdzie średnia μ_Y jest określona jako 6.16:

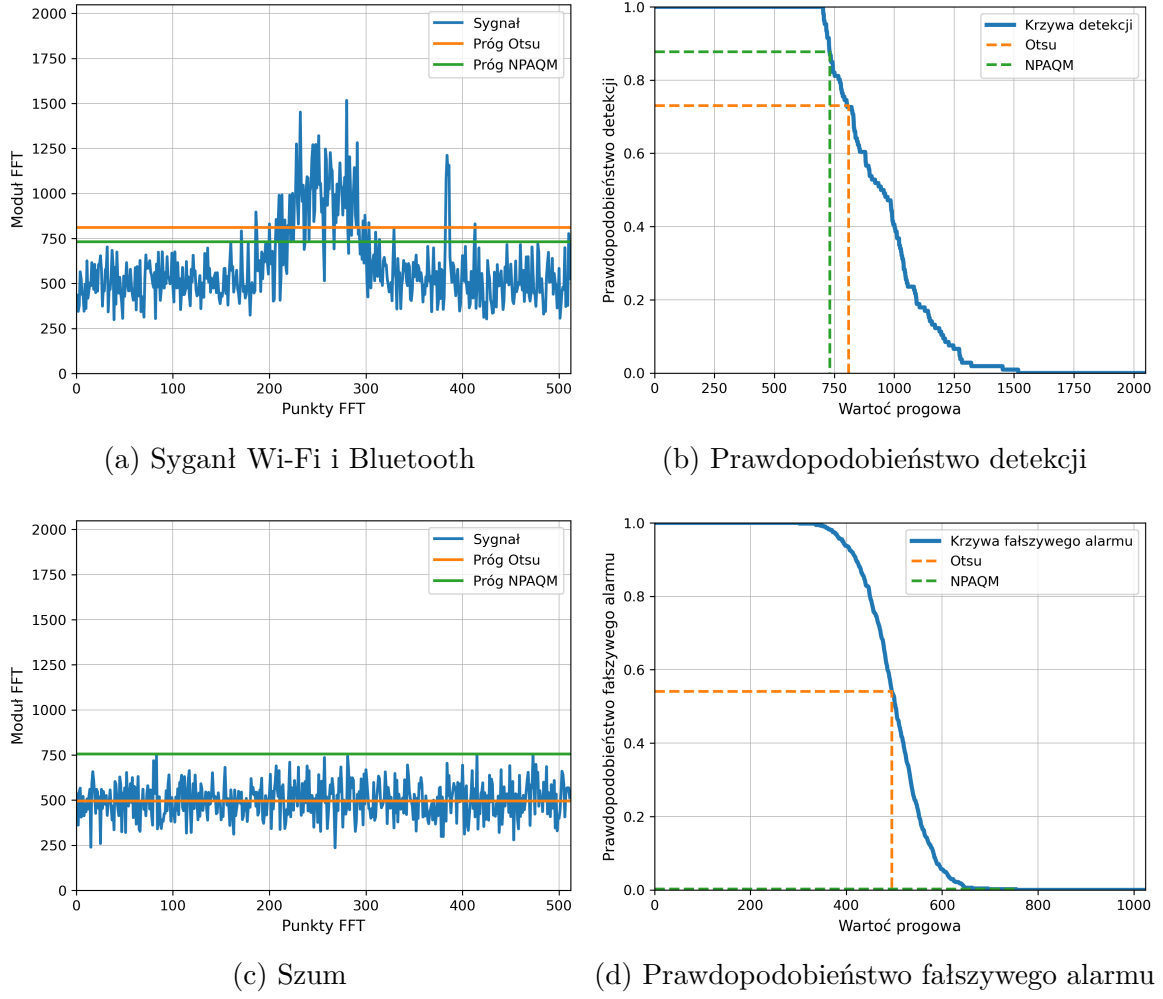
$$\mu_Y = \frac{1}{L} \sum_{l=1}^L Y_l, \quad (6.16)$$

i wtedy próg przyjmuje wartość maksymalnej próbki ze zbioru. Przykładową wartość obliczonego progu dla NPAQM w zestawieniu z podstawową metodą Otsu prezentuje rysunek 6.6.

Progowanie przebiegu jest jednym z kroków przeprowadzanych w celu finalnej detekcji krawędzi, zamknięcia wykrytych ramek w struktury prostokątne i przekazania ich do fazy klasyfikacji. Aby rozwiązać kwestię redukcji szumów przed procesem progowania i zminimalizować współczynnik fałszywych alarmów, sprawdzono kilka architektur filtrów wygładzających, jak wcześniej było to sugerowane dla metody FCME. Wyniki prezentuje rysunek 6.7. Najlepszymi rozwiązaniami do tłumienia wysokich częstotliwości przy jednoczesnym zachowaniu krawędzi okazały się filtry Gaussa i bilateralny, które nie wpłynęły znacząco na odwzorowanie zajmowanej szerokości i długości sygnału. Proces filtrowania gaussowskiego jest jednak dużo prostszy pod względem obliczeniowym, a jego potencjalna implementacja w FPGA nie wymaga użycia komórek mnożących. Funkcję filtra $G(x, y)$ dla przypadku dwuwymiarowego można opisać wzorem 6.17:

$$G(x, y) = S(x, y) \otimes k(x, y), \quad (6.17)$$

gdzie $\otimes$ oznacza konwolucję, $k(x, y)$ jest funkcją maski, a $S(x, y)$ sygnałem wejściowym. W domenie cyfrowej, dyskretna maska tworzy macierz o rozmiarze $n \times n$, z promieniowo symetrycznymi współczynnikami. Różne rozmiary maski i ich wpływ na proces wykrywania sygnału będą dalej badane eksperymentalnie. Przykładową maskę $k(x, y)$ dostosowaną do



Rysunek 6.6: Prezentacja obliczeń wartości progowej dla algorytmu Otsu i NPAQM wraz z krzywymi detekcyjnymi.

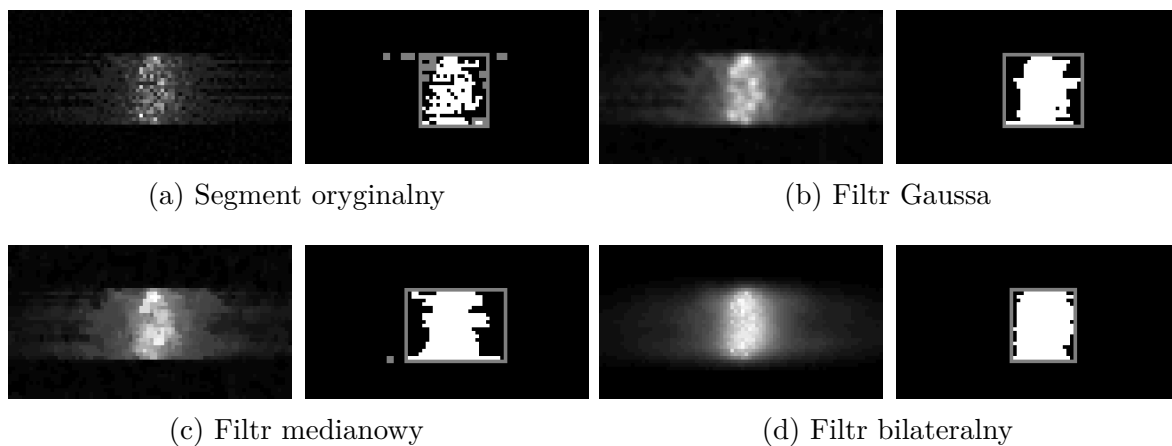
obliczeń w sprzęcie, można wyrazić jako 6.18:

$$k(x, y) = \frac{1}{16} \begin{bmatrix} 1 & 2 & 1 \\ 2 & 4 & 2 \\ 1 & 2 & 1 \end{bmatrix}. \quad (6.18)$$

Finalnie, przed uruchomieniem funkcji poszukiwania konturów wykorzystującej algorytm z biblioteki OpenCV [179], wprowadzono dodatkowe operacje morfologiczne. Proces erozji może wyeliminować szum, podczas gdy dyatacja potrafi następnie przywrócić nieprawidłowo wyeliminowane obszary spektrogramu. Biorąc pod uwagę spektrogram jako A , a maskę jako B w zbiorze pikseli Z^2 , dyatację można wyrazić jako 6.19, a erozję jako 6.20:

$$A \oplus B = \{z | [(\hat{B})_z \cap A] \subseteq A\}, \quad (6.19)$$

$$A \ominus B = \{z | (B)_z \subseteq A\}. \quad (6.20)$$



Rysunek 6.7: Różne algorytmy filtrowania zastosowane do segmentu spektrogramu i odpowiadające im wyniki procesu doboru prostokąta ograniczającego.

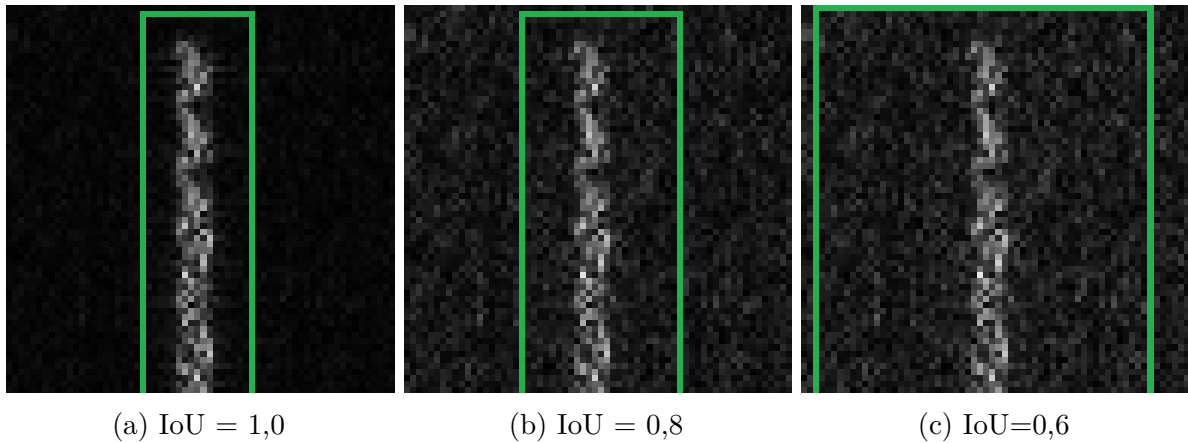
Gdy obie metody są połączone, następuje nieliniowe filtrowanie czasowo-częstotliwościowe. Zarówno erozja, jak i dylatacja są procesami, które mogą być używane wielokrotnie, ale żadna z tych procedur nie jest odwracalna. Celem otwarcia morfologicznego jest rozszerzenie erodowanego fragmentu i przywrócenie jak największej części oryginału, a zamknięcie jest operatorem do niego dualnym. Procesy te potrafią również łączyć drobne pęknięcia i długie, cienkie szczeliny, wypełniać luki i eliminować małe ubytki w obrazie widma. Dobór kolejności zastosowania tych operacji jest badany eksperymentalnie, a procesy otwarcia i zamknięcia można zapisać odpowiednio jako 6.21 oraz 6.22:

$$A \circ B = (A \ominus B) \oplus B, \quad (6.21)$$

$$A \bullet B = (A \oplus B) \ominus B. \quad (6.22)$$

Praca detektora zbadana została przy wykorzystaniu rzeczywistego nagrania sygnału modelowego drona. Zapisy te uzupełniono programowo o kanał AWGN dla stworzenia eksperymentalnej bazy sygnałowej w zakresie od -10 dB do 20 dB SNR. Przy wysokim SNR określony został wzorzec idealnej ekstrakcji ramki, do którego odniesiono każdy kolejny wynik pracy algorytmu. Aby ocenić jakość każdej detekcji, wykorzystano wskaźnik Jaccarda, określane także jako IoU (ang. *Intersection-over-Union*). Metryka ta definiowana jest jako proporcja nakładania się rzeczywistej lokalizacji ramki i przewidywanej jej pozycji w spektrogramie. Współczynnik IoU można wyznaczyć jako stosunek części wspólnej pola obiektu wyznaczonego przez algorytm i pola obiektu wyznaczonego przez wzorzec do sumy tych pól.

Przykładowe poziomy IoU dla sygnałów sterujących komercyjnym systemem bezzałogowym, gdzie wraz ze spadkiem SNR przewidywany obszar rośnie, przedstawione są na rysunku 6.8. Eksperymentalny dobór maski filtra Gaussa jest przedstawiony w odniesieniu do progów IoU 0,6 i 0,8 na rysunku 6.9. Pokazano tutaj, że nawet przy dodatnim SNR

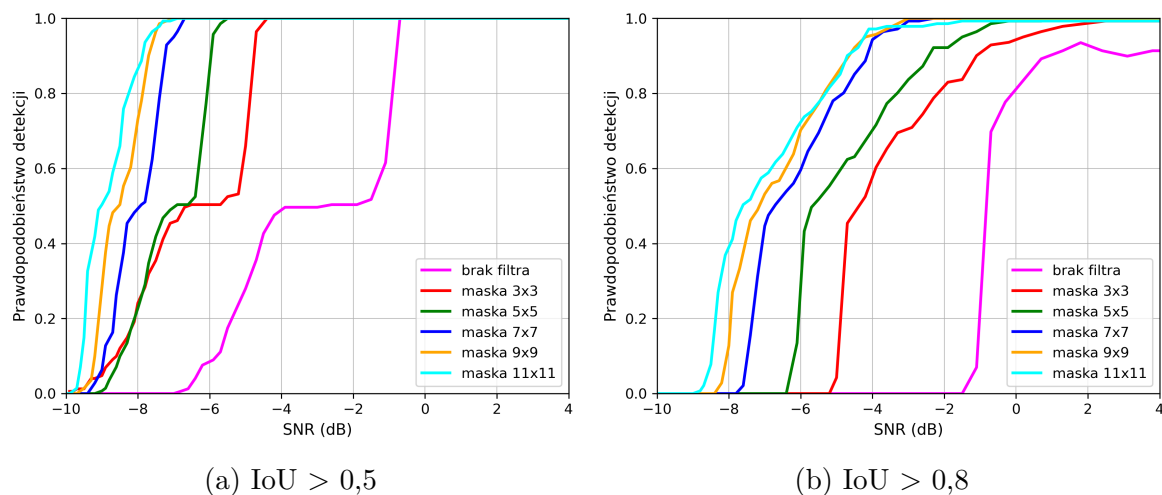


Rysunek 6.8: Przykładowe wartości parametru IoU dla pola ograniczającego wykrytą transmisję radiową, wyświetlane na wyciętych obszarach spektrogramu.

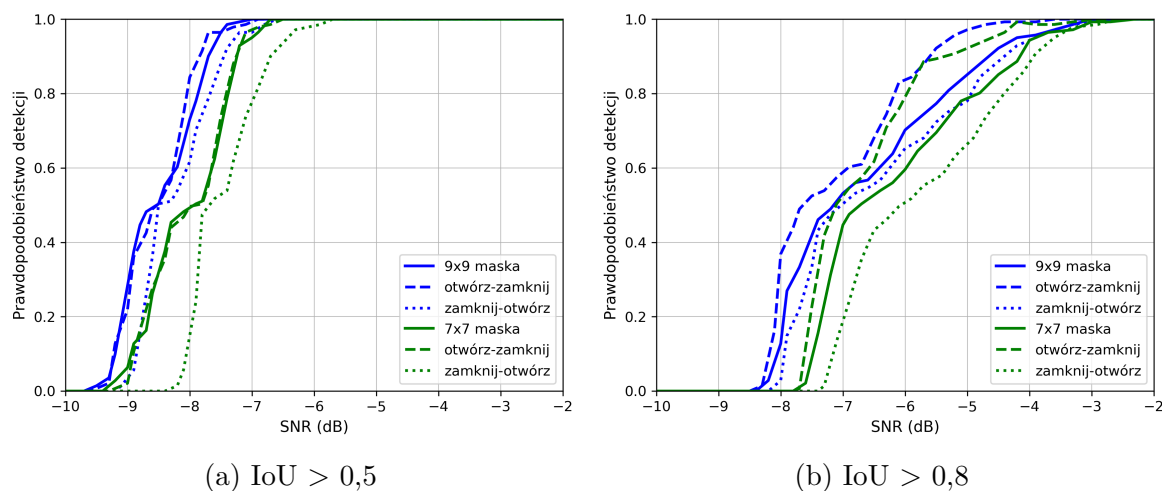
przy braku jakiegokolwiek filtra wygładzającego, dokładność detektora spada szybko dla sygnałów poniżej 0 dB. Dokładność jednak poprawia się nawet przy ujemnym SNR wraz ze wzrostem rozmiaru maski. Dodatkowo, ponieważ krzywa detekcji stopniowo się nasycza, zwiększenie jej rozmiaru powyżej 9×9 nie przynosi znaczących korzyści. Właściwa kolejność stosowania operatorów morfologicznych doprowadziła do dalszej poprawy, jak widać na rysunku 6.10. Przedstawiono tu wpływ zmiany kolejności ich użycia, odniesioną do sytuacji całkowitego braku ich stosowania. Dla obu przypadków IoU, kolejność funkcji, gdzie najpierw stosuje się otwieranie, a potem zamykanie, po zastosowaniu filtracji i progowania, dała wyniki średnio o około 0,5 dB lepsze dla zakresu ujemnych SNR i IoU 0,8. Dodatkowo dokładność na poziomie 0,99 utrzymała się nawet do -4,5 dB SNR, przesuwając tę granicę z poziomu -3,5 dB dla opcji bez operacji morfologicznych. Natomiast dla przyjętego parametru IoU 0,5, poprawa wyników nie przekroczyła 0,25 dB. Podsumowując, proponowane podejście do detekcji, które opiera się na analizie spektrogramu i wykrywaniu pojedynczej ramki radiowej, oferuje ponad 150 możliwości detekcji na sekundę dla typowego modelu drona, z uwagi na ciągły charakter jego transmisji. Nawet jeśli niektóre ramki pozostaną niewykryte, dokładność 20% osiągnięta przy -8,2 dB SNR nadal daje duży potencjał do identyfikacji niepożądanych obiektów na tej podstawie na dalszym etapie obróbki danych.

6.2.2 Klasyfikacja binarna

W bazowym systemie bezprzewodowej komunikacji cyfrowej nadajnik odpowiedzialny jest za generowanie sygnału, a funkcją odbiornika jest między innymi korygowanie częstotliwości oraz przesunięcia fazowego między lokalnymi i zdalnymi generatorami zegarowymi, co wymaga zastosowania skomplikowanych procedur. Większość powszechnie znanych systemów bezprzewodowych działających w paśmie ISM, takich jak Bluetooth i Wi-Fi, wykorzystuje algorytmy oparte na założeniu, że część przesyłanych danych jest znana.

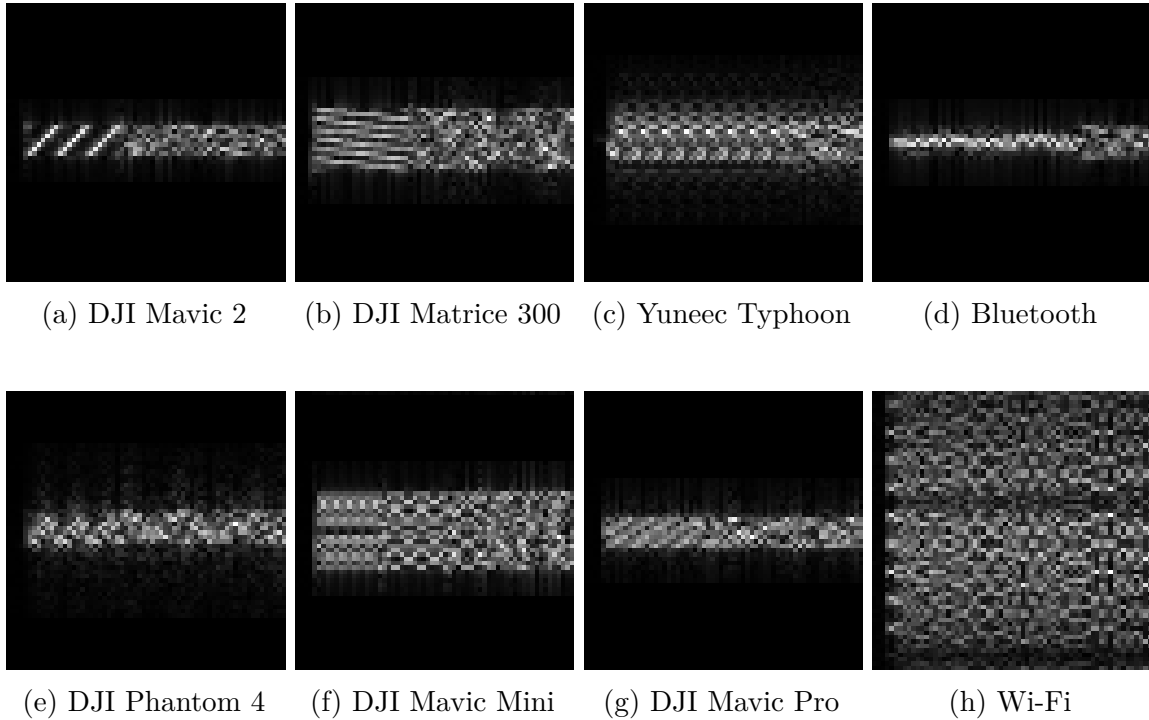


Rysunek 6.9: Prawdopodobieństwo detekcji w funkcji SNR dla różnych parametrów maski filtra gaussowskiego, w odniesieniu do przebiegu bez filtra.



Rysunek 6.10: Prawdopodobieństwo detekcji w funkcji SNR obrazujące wpływ stosowania operacji morfologicznych i ich kolejności.

Gdy sekwencja tych charakterystycznych symboli, zazwyczaj o wysokich właściwościach korelacyjnych, jest umieszczana przed samą wiadomością, nazywana jest preambułą. Sekwencja ta jest jednolita i niezależna od danych, może być więc używana do identyfikacji protokołów w paśmie ISM, a także do rozróżniania sygnałów dronów. Przykładowe wycinki widm pokazujące preambuły dla danych sygnałów, przedstawione są na rysunku 6.11. W wielu badaniach spektrogram stworzony z całej szerokości pasma ISM 2,4 GHz był zazwyczaj skalowany w dół przed przystąpieniem do aplikacji metod uczenia maszynowego. W przeciwieństwie do tego, proponowane podejście opiera się na klasyfikacji tylko wycinka spektrogramu, bez jego przekształcania. Ze względu na znacznie mniejszy rozmiar danych wejściowych, stanowi to okazję do optymalizacji modelu uczenia maszynowego dla komputerów wbudowanych. Za podstawową jednostkę poddawaną klasyfikacji przyjęto



Rysunek 6.11: Przykładowe preambuły badanych sygnałów w wycinku spektrogramu o rozmiarze 64 na 64 piksele.

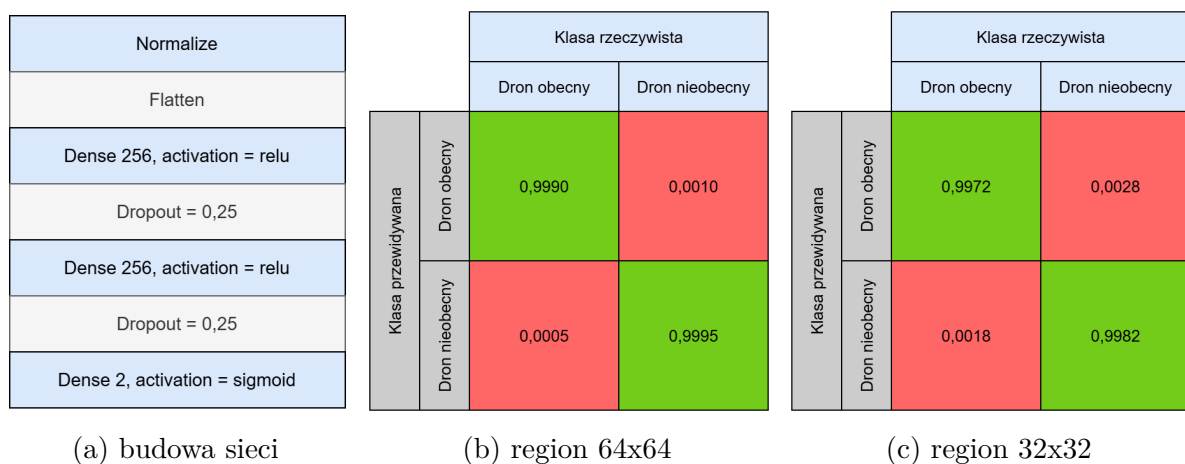
wycinek spektrogramu o rozmiarze 64 na 64 piksele, co dla 512 punktów FFT i 96 MHz częstotliwości próbkowania daje obszar obrazowania odpowiadający 12 MHz o czasie trwania 0,34 ms. Alternatywnie przebadano także opcje zmniejszenia obszaru do rozmiaru 32 na 32 piksele, co przekłada się na zakres 6 MHz i czas 0,17 ms.

Głównym wyzwaniem w tej strategii jest zapewnienie całościowego obrazu widma przy jednoczesnym wykorzystaniu dużej częstotliwości próbkowania i długości transformaty czasowo-częstotliwościowej zapewniającej niezbędną rozdzielczość. Aby uniknąć rozmycia sygnału właściwego, niewskazane jest także stosowanie uśredniania kolejnych ramek FFT, aby nie zatracić indywidualnego wzorca początku ramki. Ponadto strumień danych z SDR nie może zawierać strat pakietów ze względu na możliwość pominięcia lub przzerwania wzorca preambuły. Te aspekty zostały spełnione dla założonej architektury przedstawionego fizycznego prototypu sensora.

Weryfikacja proponowanego podejścia rozpoczęła się od budowy bazy sygnatur radiowych dla sygnałów, które występują w pasmach ISM. W tym celu, w pierwszej kolejności posłużono się laboratoryjnymi nagraniami dronów zaczerpniętymi z otwartego zbioru opisywanego wcześniej [173]. W każdym z przebiegów oszacowany został SNR, a następnie na wszystkie nagrania nałożony został szum w celu symulacji wartości tego parametru do poziomu -10 dB, z krokiem około 0,5 dB. Dodatkowo, baza ta uzupełniona została o sygnały Wi-Fi oraz Bluetooth wygenerowane w środowisku Matlab, z parametrem SNR od 20 dB do -10 dB, co 0,5 dB. Podczas tego procesu zachowano tę samą częstotliwość próbkowania

Tabela 6.1: Wyniki klasyfikacji binarnej dla różnych modeli oparte na metodzie analizy wycinka spektrogramu

Model 32	Dokładność	Miara F1	Czas
KNN	0,9851	0,9862	0,036 ms
DT	0,9650	0,9876	0,059 ms
RDF	0,9896	0,9821	0,038 ms
ANN	0,9978	0,9963	0,035 ms
Model 64	Dokładność	Miara F1	Czas
KNN	0,9965	0,9967	0,112 ms
DT	0,9764	0,9968	0,091 ms
RDF	0,9931	0,9931	0,119 ms
ANN	0,9993	0,9992	0,089 ms



Rysunek 6.12: Architektura zastosowanej sieci wraz z wynikami klasyfikacji binarnej dla różnego rozmiaru regionu.

dla sygnałów wygenerowanych, jak i nagranych w laboratorium. Te dodatkowe przebiegi, w każdym kroku SNR, zawierały po 100 ramek dla każdej transmisji: 802.11ax, 802.11n/ac, Bluetooth 2.0 i Bluetooth Low Energy. Cały zbiór danych został oznaczony oraz losowo podzielony na zestawy treningowe, walidacyjne i testowe w stosunku 7:2:1. Przy użyciu tak utworzonej bazy danych przetestowane zostały różne modele uczenia maszynowego, dla obu rozmiarów wybieranego obszaru, co podsumowane jest w tabeli 6.1. Struktura zastosowanej sieci neuronowej oraz jej macierz pomyłek przedstawione są szczegółowo na rysunku 6.12.

W zestawieniu widać, iż prosta sieć neuronowa daje najlepsze wyniki pod względem dokładności oraz czasu obliczeń w klasyfikacji binarnej. Porównując ze sobą rezultaty oparte na sieciach o różnym formacie wejściowym, można zauważyć, iż wersja z ramką o rozmiarze 32 na 32 piksele oferuje czas obliczeń o 0,54 ms krótszy przy ogólnym spadku dokładności o 0,15%. Parametry dobranej do celów tej analizy prostej sieci, składającej się z dwóch

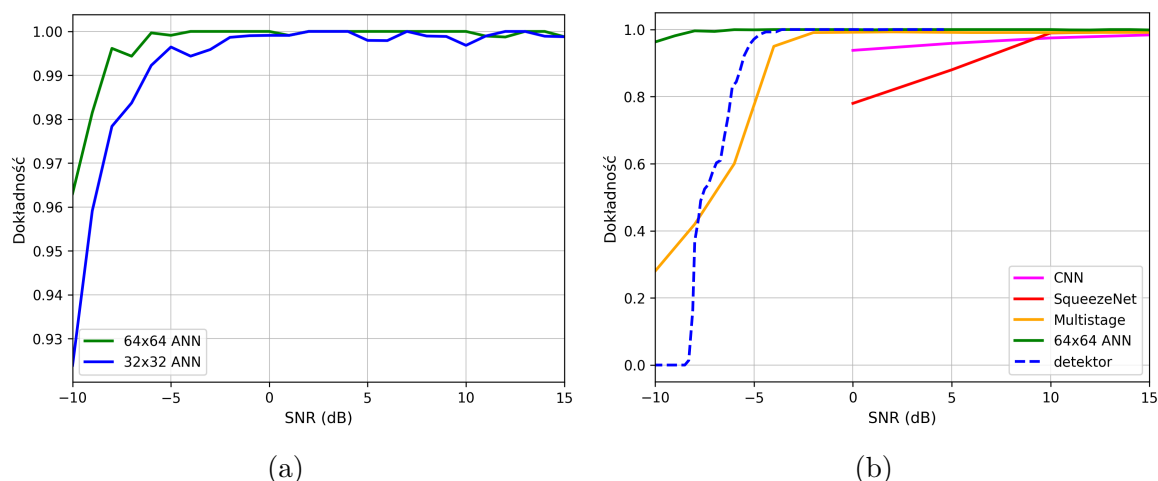
Tabela 6.2: Wyniki klasyfikacji binarnej oraz parametry zastosowanych sieci neuronowych wraz z czasem wykonywania obliczeń.

Model 64	Dokładność	Miara F1	Parametry	MFLOP	Czas
DNN [121]	0,9992	0,9991	1,09 M	2,18	0,12 ms
CNN [180]	0,9986	0,9987	0,37 M	12,48	0,22 ms
CNN [129]	0,9987	0,9988	2,19 M	82,51	0,61 ms
ANN	0,9993	0,9994	1,12 M	2,23	0,09 ms

wewnętrznych warstw w pełni połączonych o 256 neuronach, odniesione zostały także do innych struktur opisanych w tożsamyh pracach. W tym celu warstwy wejściowe i wyjściowe różnych modeli dostosowano do techniki klasyfikacji wycinka widma o rozmiarze 64 na 64 piksele. Zaobserwowane różnice w parametrach trenowalnych i milionach operacji zmiennoprzecinkowych na sekundę (ang. *Milion Floating Point Operations Per Second*, MFLOP), niezbędne do analizy złożoności obliczeniowej, przedstawiono w tabeli 6.2.

Budowa pierwszej z porównywanych sieci opiera się na trzech warstwach w pełni połączonych z odpowiednio 256, 128 i 64 neuronami [121]. Ma ona nawet mniej parametrów trenowalnych i niższe szacowane zapotrzebowanie na MFLOP niż sieć proponowana, niemniej jednak trzywarstwowa architektura sprawia, iż czas obliczeń jest dłuższy oraz występuje szcążtkowa utrata dokładności dla klasyfikacji binarnej. W wersji pierwotnej sieć przeznaczona była do klasyfikowania wektora o rozmiarze 2048 na 1 w dziedzinie częstotliwości i posiadała 0,57 M parametrów trenowalnych przy 1,13 MFLOP. Kolejna sieć, w której oryginalne podejście oparte jest na pełnym spektrogramie, bazuje tylko na trzech warstwach konwolucyjnych, z odpowiednio 64, 128 i 256 filtrami [180]. Pierwotnie cechuje ją 0,485 M parametrów trenowalnych przy 507,9 MFLOP dla tensora wejściowego o rozmiarze 356 na 452. Ta sama struktura sieci ze zmniejszonym tensorem wejściowym pozwala na redukcję parametrów do 0,39 M i 213,4 MFLOP. Architektura tę jednak cechuje spadek dokładności i wzrost czasu przetwarzania. W ostatniej sieci, do trzech warstw konwolucyjnych składających się odpowiednio z 32, 64 i 128 filtrów, dodano jedną warstwę głęboką z 256 neuronami [129]. Pierwotnie przeznaczona jest ona do klasyfikacji spektrogramów o rozmiarze 90 na 380 pikseli. W oryginalnej wersji posiada 17,03 M trenowalnych parametrów i wymaga 720,15 MFLOP. Mimo swojej skomplikowanej budowy, sieć nie daje najlepszych wyników, mimo najdłuższego czasu wymaganego do obliczeń.

Dalsza analiza dotycząca dokładności proponowanego podejścia w odniesieniu do SNR przedstawiona jest na rysunku 6.13a, gdzie można zauważyć, iż największy wpływ na jej utratę w obu przypadkach ma obszar SNR od -3 dB do -10 dB. Proponowana metoda odniesiona została także całościowo do innych opracowań, w których udało się odnaleźć zależność dokładności detekcji od SNR, co zaprezentowane jest na rysunku 6.13b. Podejście przedstawione w [119], oznaczone jako CNN, operuje na surowych sygnałach w dziedzinie czasu podawanych bezpośrednio do modelu sieci i nie wymaga żadnych technik ekstrakcji



Rysunek 6.13: Podsumowanie wyników pracy metody dwuetapowej w odniesieniu do SNR: (a) dokładność klasyfikacji dla obu rozmiarów pola danych, (b) zestawienie charakterystyk wybranej sieci z technikami innych autorów i skutecznością detektora.

cech. Model wytrenowany z danymi od 0 dB do 30 dB SNR osiąga średnią dokładność 97,53%. Kolejna technika [181] wykorzystuje transformatę falkową, która wykorzystuje zmienną funkcję okna, w przeciwieństwie do STFT. Autorzy zastosowali model uczenia maszynowego SqueezeNet, który osiągnął dokładność 98,9% przy SNR 10 dB. W innym systemie [33] zaimplementowano wieloetapowy detektor, w którym zastosowano zestaw 15 parametrów statystycznych w celu opisanie ramki radiowej drona zarówno w dziedzinie czasu, jak i częstotliwości. Przy SNR 10 dB dokładność wykrywania wyniosła 99,8%, a współczynnik fałszywych alarmów 2,8%. Dla porównania, proponowana struktura zachowuje ponad 96% dokładności rozróżnienia transmisji dronowych od Wi-Fi i Bluetooth w całym prezentowanym zakresie SNR. Całościowo jednak ograniczenie wprowadza tutaj faza detekcji, gdyż sygnały poniżej -9 dB SNR nie przejdą nawet do fazy klasyfikacji binarnej.

6.2.3 Detekcja i klasyfikacja jednorodna

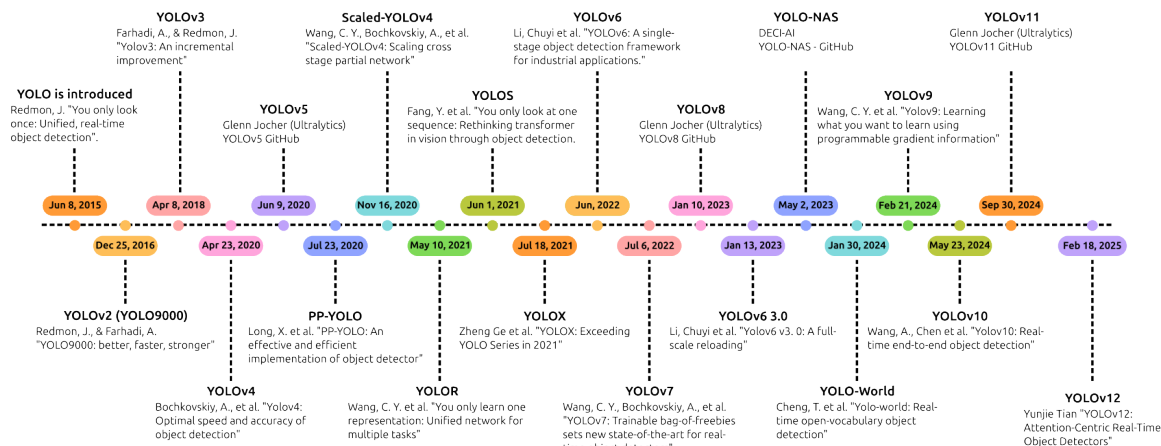
Wykrywanie obiektów przy użyciu zaawansowanych technik uczenia maszynowego można generalnie podzielić na dwie kategorie. Wyróżnić tu można detektory jednostrzałowe (ang. *single-shot detectors*) i detektory wielostrzałowe (ang. *multi-shot detectors*). W obu przypadkach proces detekcji rozpoczyna się od przyjęcia obrazu na wejściu i ekstrakcji cech, a elementem modelu odpowiedzialnym za tę funkcję jest tak zwany kręgosłup (ang. *backbone*). Cechy głębokie stanowią pojedynczy wektor lub siatkę wektorów liczbowych, tworzących mapę cech, a pozyskiwane są w procesie trenowania modelu. Na tym etapie przechwytywane są proste wzorce, takie jak krawędzie i tekstury, a wybór odpowiedniego podejścia uzależniony jest od konkretnych warunków pracy modelu. Obecnie często używa się sieci takich jak ResNet czy DarkNet, a rozwiązania takie jak MobileNet

czy EfficientNet oferują także możliwość optymalizacji złożoności obliczeniowej kosztem skuteczności, z uwagi na dostępność całej serii modeli o różnych parametrach. Kolejnym elementem, który możemy często odnaleźć w strukturach złożonych sieci, jest szyja (ang. *neck*), która stanowi pomost pomiędzy opisanym wcześniej kręgosłupem a głowicą lub głową (ang. *head*). Wykonuje ona operacje fuzji cech i integracji informacji kontekstowych. Dodatkowo może zmniejszyć rozdzielczość przestrzenną i wymiarowość zasobów w celu ułatwienia obliczeń. Głowica natomiast jest końcową warstwą sieci odpowiedzialną za przygotowanie danych wyjściowych, takich jak ramki ograniczające i dopasowane do nich poziomy ufności (ang. *confidence scores*) wskazujące prawdopodobieństwo obecności wykrytego obiektu [182].

Detektory jednostrzałowe przewidują obwódnię i klasę obiektu w jednym przebiegu, a proces ten przeprowadzany jest bezpośrednio na danych wyjściowych z ekstraktora cech. Głowica w tym przypadku może składać się z dwóch osobnych podsieci, jednej do określania klas, a drugiej do wyznaczania prostokątów ograniczających wykryte obiekty. Zadanie to może być także wykonane przez jedną, niekorzystającą z warstw głębokich, wielozadaniową sieć konwolucyjną. Architektury te są bardzo szybkie i wydajne, odpowiednie do zadań wymagających realizacji w czasie rzeczywistym. Detektory wielostrzałowe stosują natomiast dwuetapowy proces, w którym pierwszy krok polega na zaproponowaniu serii obszarów, które mogą potencjalnie zawierać obiekt. Często odbywa się to przy użyciu metody zwanej propozycją regionu (ang. *Regions of Interest*). W kroku drugim natomiast wyekstrahowane obszary poddawane są klasyfikacji przez dalsze warstwy sieci neuronowej. Proces ten może być powtarzany wielokrotnie, co znacznie wydłuża działanie algorytmu, ale także zwiększa jego dokładność. W ten sposób złożoność obliczeniowa fazy drugiej staje się wrażliwa na dane wejściowe, co utrudnia finalny szacunek czasu przetwarzania. Funkcją głowicy w tej architekturze jest nie tylko klasyfikacja i lokalizacja, ale i dla sieci, które wykonują zadanie segmentacji, generowanie masek wykrytych obiektów. Przykładem realizacji tych funkcji jest rodzina sieci znana jako R-CNN (ang. *Region-based Convolutional Neural Network*) [182].

Najpopularniejszym reprezentantem kategorii jednostrzałowej jest rodzina sieci YOLO (ang. *You Only Look Once*)[183], która od wprowadzenia w 2015 roku stała się szeroko stosowana do tworzenia detektorów obiektów w czasie rzeczywistym, nie tylko w dziedzinie rozpoznawania obrazów, ale także w analizie spektrogramów [184, 185, 186]. Do 2025 roku architektura ta ewoluowała przez dwanaście głównych wersji, podczas gdy twórcy oryginału opracowali trzy pierwsze, a kolejne rozwinięte zostały już przez różne zespoły w ramach aktywnej społeczności. Ścieżka rozwoju tego podejścia zaprezentowana jest na rysunku 6.14. Przy zachowaniu podstawowej koncepcji YOLO wiele rozwijanych edycji integruje innowacyjne techniki i zmiany architektoniczne w celu dalszej poprawy wydajności modelu oraz jakości wnioskowania.

Chociaż te udoskonalenia są istotne, nie zawsze przekładają się na znaczącą poprawę



Rysunek 6.14: Ścieżka ewolucji sieci z rodziny YOLO [187].

w szerszym kontekście zadań wykraczających poza standardową bazę testową COCO (ang. *Common Objects in Context*). Na przykład w badaniu dotyczącym liczenia kłosów pszenicy, YOLOv7 osiągnął lepsze wyniki niż YOLOv8, podczas gdy w wykrywaniu podwodnych rurociągów YOLOv5 osiągnął lepsze wyniki niż YOLOv6, YOLOv7 i YOLOv8. Podobnie, badanie dotyczące zagrożeń w posługiwaniu się nożem kuchennym wykazało, że YOLOv5 i YOLOv8 cechowały się wyższą dokładnością niż YOLOv10, podczas gdy YOLOv10 miał najwyższy wskaźnik błędnej klasyfikacji [188]. Kompleksowe porównanie modeli z rodziny YOLO oraz ocena ich wydajności przedstawiona została w opracowaniu [187]. W tym przypadku nie opierano się na bazie COCO, a zestawy danych zostały dobrane tak, aby obejmować różne właściwości obiektów, w tym rozmiary, proporcje i gęstość rozmieszczenia. W rezultacie seria YOLO11 okazała się najbardziej wszechstronna, a model YOLO11m osiągnął optymalną równowagę między dokładnością, wydajnością i rozmiarem modelu. Seria YOLOv10 zapewniła nieznacznie niższą dokładność niż YOLO11, jednakże wyróżniła się szybkością i wydajnością. Linia YOLOv9, osiągając także zadowalające wyniki, szczególnie wyróżniała się w odniesieniu do mniejszych zbiorów danych. Sieci z kategorii YOLO12 natomiast, pomimo że są najnowszymi przedstawicielami rodziny, zaprezentowały rozczarowującą wydajność. Ambitne zmiany architektoniczne wprowadziły tu dodatkowe poziomy złożoności, nie przekładając się na wyraźne korzyści, co spowodowało zachwianie równowagi między dokładnością a szybkością.

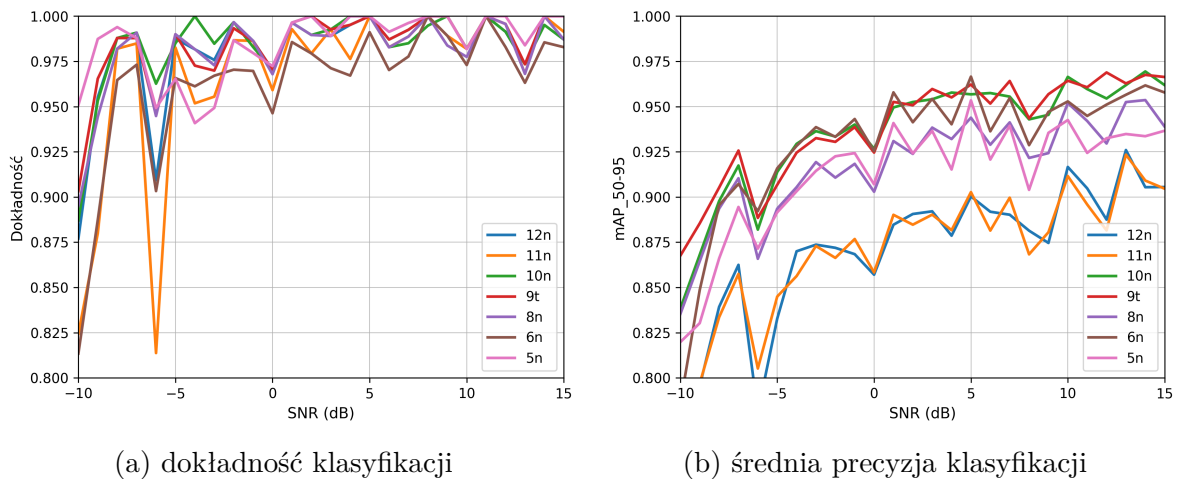
Dla porównania różnych modeli YOLO w zadaniu przetwarzania spektrogramu, jakość wykrywania obiektów określona została przy użyciu podstawowych wskaźników, jakimi są dokładność i miara F1. Nowym parametrem jest tutaj natomiast średnia precyzja (ang. *Mean Average Precision*, mAP), wyznaczona dla każdej klasy przez obszar pod krzywą precyzja-czułość, a następnie uśredniona między poszczególnymi klasami. Metryka ta badana jest zazwyczaj dla dwóch progów IoU, wynoszących odpowiednio 50% i dla zakresu od 50% do 95%, w celu dostarczenia pojedynczej wartości zapewniającej kompleksową ocenę modelu. Wszystkie eksperymenty odbywały się na źródłowym zestawie testowym

Tabela 6.3: Parametry sieci z edycji YOLO 5 do 12.

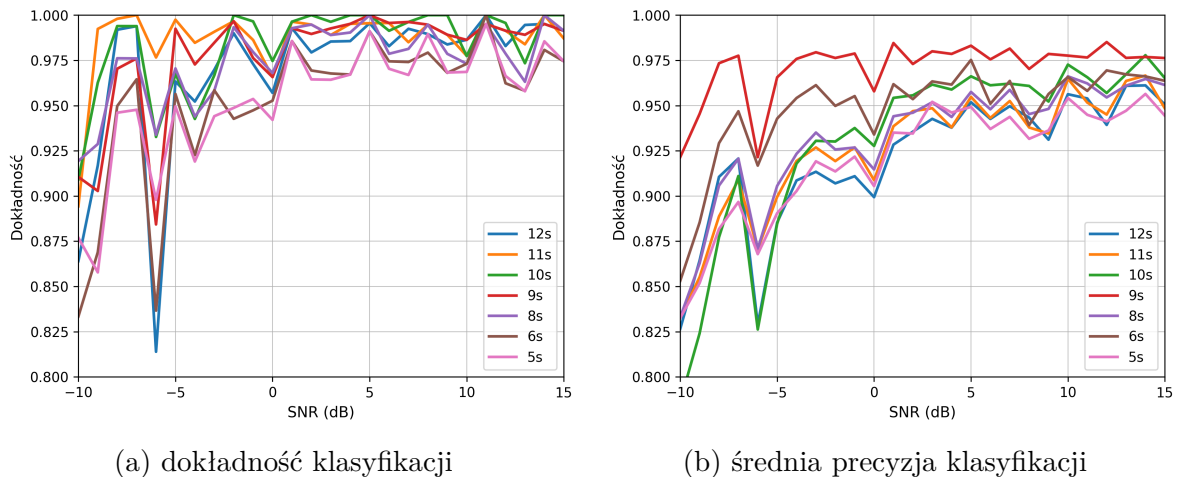
Model	Dokładność	Miara F1	mAP50	mAP50-95	Parametry	GFLOP	Czas
YOLO12n	0,9836	0,9937	0,9947	0,8697	2,6 M	6,5	67,5 ms
YOLO11n	0,9659	0,9864	0,9938	0,8734	2,6 M	6,5	58,5 ms
YOLOv10n	0,9861	0,9951	0,9949	0,9374	2,3 M	6,7	57,5 ms
YOLOv9t	0,9864	0,9956	0,9945	0,9412	2,0 M	7,7	68,7 ms
YOLOv8n	0,9829	0,9946	0,9948	0,9208	3,2 M	8,7	50,8 ms
YOLOv6n	0,9642	0,9947	0,9946	0,9358	4,2 M	7,7	49,3 ms
YOLOv5n	0,9852	0,9945	0,9947	0,9137	2,5 M	7,7	46,2 ms
YOLO12s	0,9700	0,9891	0,9945	0,9252	9,3 M	21,4	107,4 ms
YOLO11s	0,9891	0,9967	0,9949	0,9282	9,4 M	21,5	97,2 ms
YOLOv10s	0,9851	0,9939	0,9949	0,9323	8,0 M	24,8	98,6 ms
YOLOv9s	0,9791	0,9929	0,9941	0,9759	7,3 M	27,4	153,7 ms
YOLOv8s	0,9760	0,9940	0,9945	0,9342	11,1 M	28,6	111,2 ms
YOLOv6s	0,9514	0,9920	0,9934	0,9508	16,3 M	44,2	132,8 ms
YOLOv5s	0,9520	0,9877	0,9941	0,9220	9,1 M	24,0	98,9 ms

znany z poprzednich sekcji, z podziałem bazy w stosunku 7:2:1, a wyniki przedstawione są dla najlepszego przebiegu po 200 epokach treningu. Utrzymano tutaj także koncepcję opierającą się na wykrywaniu tylko preambuły sygnału, z tą różnicą w stosunku do stałego pola 64 na 64 piksele, że dla każdego typu transmisji została ona indywidualnie dopasowana i oznaczona. Za podstawową jednostkę poddawaną klasyfikacji przyjęto kwadratowy obraz najbardziej zbliżony do natywnego rozmiaru wejściowego sieci YOLO, który wynosi 640 pikseli. Cały obraz widma o pełnej szerokości 512 punktów FFT może być tym samym klasyfikowany w jednym momencie, a zachowanie proporcji dla 96 MHz częstotliwości próbkowania tworzy wycinek spektrogramu o czasie trwania 2,7 ms.

W serii eksperymentów porównano ze sobą modele YOLO różnych generacji oraz o różnym stopniu gęstości sieci. Rozróżnienie to zaczęło pojawiać się od piątej edycji serii, aby lepiej dopasować modele do możliwości sprzętowych. W pierwszej kolejności zestawiono ze sobą sieci o najmniejszej gęstości dla każdej edycji od dwunastej do piątej, z wyłączeniem siódmej, w której optymalizacja dotyczyła bardziej procesu trenowania niż architektury. Uzupełnione to zostało także testami modeli o stopniu skomplikowania o jeden poziom wyżej od podstawowego. Zestawienie wyników dla poszczególnych modeli podsumowano w tabeli 6.3. Poza parametrami samej sieci, zawarto tam czas przetwarzania dla referencyjnego sprzętu oraz miary jakości klasyfikacji. Wartości czasowe zmierzono na sprzęcie zgodnym z poprzednimi eksperymentami przeprowadzonymi w tym rozdziale. Aby wskazać na więcej szczegółów, próbki z przedziału testowego posortowane zostały zgodnie z odpowiednimi przedziałami SNR i ponownie poddane walidacji. Wyniki dla sieci o najmniejszej gęstości zaprezentowano na wykresie 6.15, a dla sieci o wyższym stopniu skomplikowania na wykresie 6.16.



Rysunek 6.15: Podsumowanie wyników działania modeli z rodziny YOLO dla wersji sieci o najniższej gęstości w odniesieniu do SNR.



Rysunek 6.16: Podsumowanie wyników działania modeli z rodziny YOLO dla wersji sieci o większej gęstości w odniesieniu do SNR.

Wśród sieci z kategorii pierwszej pod względem parametrów jakościowych najlepiej sprawdziła się YOLOv9t, jednakże nastąpiło to kosztem najdłuższego w tej grupie czasu przetwarzania. Dla modelu YOLOv10n spadek dokładności w stosunku do YOLOv9t jest minimalny, a miara mAP50 okazała się tu nawet wyższa, przy czasie przetwarzania krótszym o ponad 10 ms, co czyni go najlepiej zbalansowanym rozwiązaniem. W zestawieniu tym sieci z najnowszych edycji YOLO12n oraz YOLO11n wypadły najgorzej pod względem miary mAP50-90, co dodatkowo uwidocznione jest na wykresie uwzględniającym SNR. Sieć YOLOv5n, która miała najkrótszy czas przetwarzania, mimo słabego wyniku miary mAP50-90, wykazała najlepszą dokładność w przedziale SNR od -7 dB do -10 dB.

Wśród sieci z kategorii drugiej największą dokładność przy najkrótszym czasie przetwarzania w grupie uzyskała sieć YOLO11s, co szczególnie uwidocznione jest w przedziale SNR od -2 dB do -10 dB. Pod względem parametrów jakościowych ustępuje ona jedynie

w mierze mAP50-95 modelowi YOLOv9s, który ponownie osiągnął tu najlepszy wynik, również kosztem najdłuższego czasu przetwarzania. Podobnie jak w poprzednim zestawieniu, sieć YOLOv10s wykazała najlepszy balans pomiędzy jakością a wydajnością.

Zestawiając ze sobą wyniki w obu grupach, nie widać znaczącej poprawy parametrów jakościowych wynikających ze stosowania modeli o większym stopniu złożoności w stosunku do tych najprostszych. Dodatkowo, charakteryzuje je średnio dwukrotnie zwiększony czas przetwarzania. Najlepsza pod względem dokładności w całym zestawieniu sieć YOLO11s ma tylko 0,27% przewagi nad YOLOv9t, przy czasie obliczeń zwiększonym o 28,5 ms i mniejszym o 1,3% parametrze mAP50-95. Dla najlepiej zbalansowanej sieci z serii YOLOv10 natomiast, mniejszy model ma przewagę we wszystkich badanych parametrach nad modelem o większej gęstości.

6.2.4 Badania w środowisku rzeczywistym

Zaawansowane sieci neuronowe przeznaczone do zadania analizy obrazu z kamery wideo, określane są jako dostosowane do pracy w czasie rzeczywistym, kiedy czas przetwarzania sceny wynosi poniżej kilkudziesięciu milisekund. Jest to spowodowane charakterystyką samego źródła obrazu, które zazwyczaj zapewnia dane z prędkością około 30 klatek na sekundę, co daje 33 ms na wykonanie inferencji. W przypadku analizy widma w czasie rzeczywistym, przy założeniu rozdzielczości spektrogramu 512 na 512 pikseli i częstotliwości próbkowania 96 MHz, odpowiada to około 370 klatkom na sekundę oraz 2,7 ms przetwarzania. Dla sieci YOLO czas w okolicy 2 ms jest wprawdzie osiągalny, jednak takie rezultaty wymagają zastosowania specjalizowanych układów graficznych. Z tego powodu do implementacji w urządzeniu wbudowanym przyjęto technikę z detektorem klasycznym i klasyfikatorem opartym na prostej sieci neuronowej.

Przygotowanie wybranej metody do zastosowania w warunkach rzeczywistych wymaga przeprowadzenia dodatkowego procesu, jakim jest transformacja modelu do postaci możliwej do uruchomienia na komputerze wbudowanym. Pierwszym krokiem tej procedury jest jego konwersja po treningu do specjalnego formatu, który początkowo utrzymuje niezmienną precyzję zmiennoprzecinkową. Operacja ta zmniejsza rozmiar zapisanego modelu dla wycinka 64 na 64 piksele z 4,25 MB do 2,9 MB, bez obniżenia dokładności. W kolejnym kroku natomiast wymagana jest kwantyzacja, polegająca na przekształcaniu zmiennoprzecinkowych 32-bitowych operacji do reprezentacji 8-bitowej. Podejście to zmniejsza opóźnienia w sieci i poprawia sprawność energetyczną, ponieważ operacje mogą być wykonywane przy użyciu typów całkowitych. Optymalizacja struktury sieci, dostosowana do wdrożenia na komputerach wbudowanych, zapewniła dalszą redukcję rozmiaru modelu do 0,6 MB kosztem utraty 0,02% dokładności w stosunku do oryginału.

Częstotliwość próbkowania w prototypowym łańcuchu detekcji wynosi 96 MHz, co znacznie różni się od tej dostępnej w otwartej bazie danych. W rezultacie konieczna

		Klasa rzeczywista	
		Dron obecny	Dron nieobecny
Klasa przewidywana	Dron obecny	1,000	0,0000
	Dron nieobecny	0,0017	0,9983

(a)

		Klasa rzeczywista	
		Dron obecny	Dron nieobecny
Klasa przewidywana	Dron obecny	0,9985	0,0015
	Dron nieobecny	0,0151	0,9849

(b)

Rysunek 6.17: Macierz pomyłek dla prototypu i algorytmu dwustopniowego w warunkach rzeczywistych dla różnych odległości nadajnika od odbiornika: (a) do 150 m, (b) do 350 m.

była budowa własnego zbioru, ponieważ wcześniej wytrenowana sieć, wykorzystywana w swojej oryginalnej formie, nie prezentowała zadowalających wyników. W tym celu na otwartej przestrzeni nagrano sygnały z sześciu modeli dronów, wraz z urządzeniami Wi-Fi i Bluetooth, bezpośrednio przy pomocy prototypowego sensora. Aby zbudować zestaw danych oddający warunki rzeczywiste, wszystkie nadajniki przemieszczano w odległości od 10 m do 350 m od urządzenia odbiorczego. Następnie dane te zostały przetworzone i oznaczone. Finalnie w odległości do 150 m odnotowano 100% skuteczność detekcji obecności statku bezzałogowego, przy 0,17% fałszywych alarmów. Dla odległości do 350 m natomiast skuteczność detekcji spadła do 99,85% przy wzroście współczynnika fałszywych alarmów do 1,51%. Pełne macierze pomyłek prezentuje rysunek 6.17.

Rozdział 7

Badania w dziedzinie przeciwdziałania

7.1 Sygnały nawigacji satelitarnej

Sygnały nawigacji satelitarnej umożliwiają precyzyjne określenie pozycji bezzałogowego statku w przestrzeni, co jest kluczowe dla poruszania się w powietrzu oraz utrzymywania stabilności. Korzystanie z tego typu nawigacji pozwala na realizację funkcji lotu wzdłuż punktów trasowych oraz trybu powrotu do bazy, a jej brak może spowodować, że dron przeprowadzi niekontrolowane manewry lub nie podąży za zaprogramowaną trasą lotu. Zagłuszanie sygnałów GNSS uważa się za jedno z największych zagrożeń dla funkcjonowania tych maszyn, gdyż jest stosunkowo proste do zrealizowania przy pomocy urządzeń łatwo dostępnych na rynku.

Niedostępność satelitarnych systemów nawigacyjnych może być także spowodowana zjawiskami naturalnymi ograniczającymi propagację fal radiowych, dlatego zazwyczaj producenci dronów programują określony sposób zachowań na tę okoliczność. W zależności od modelu może to być przerwanie realizacji lotu po zadanej trasie i zawis w oczekiwaniu na zmianę sytuacji bądź reakcję operatora, lub wręcz powolne lądowanie w miejscu wystąpienia zakłócenia. Użytkownik ma w tym momencie zazwyczaj także możliwość przełączenia trybu pracy statku bezzałogowego na sterowanie manualne, gdzie funkcję utrzymania pozycji przejmują czujniki inercyjne i barometr. Sprawne poruszanie się w tym trybie wymaga jednak doświadczenia, gdyż dron nie utrzymuje stabilnej pozycji ze względu na dryft sensorów, co skutkuje koniecznością aktywnej kontroli przez łącze sterowania. Ponadto czynność ta może być skomplikowana do przeprowadzenia w wietrznych warunkach lub na dużych wysokościach.

W większości przypadków celem zakłócania jest całkowite wykluczenie wykorzystania usług opartych na GNSS w określonym regionie. Scenariusz, w którym urządzenie zakłócające nadaje z dużą mocą, jest zazwyczaj wyraźnie identyfikowalny, a wtedy odpowiednio

Tabela 7.1: Wartość parametru JSR w różnych opracowaniach

Typ zakłócenia	JSR	Odbiornik	Tryb	Źródło
przemiatane	≈ 60 dB	DJI Mavic 2	komora	[134]
przemiatane	38 dB	uBlox 6H	rzeczywisty	[139]
przemiatane	39 dB	uBlox 8T	rzeczywisty	[139]
przemiatane	≈ 50 dB	NovAtel SpanSE	rzeczywisty	[189]
ton	≈ 55 dB	NovAtel SpanSE	rzeczywisty	[189]
ton	38 dB	model	teoretyczny	[190]
ton	47 dB	brak nazwy	pomiar	[191]
szum	41 dB	model	teoretyczny	[190]
szum	69 dB	brak nazwy	pomiar	[191]

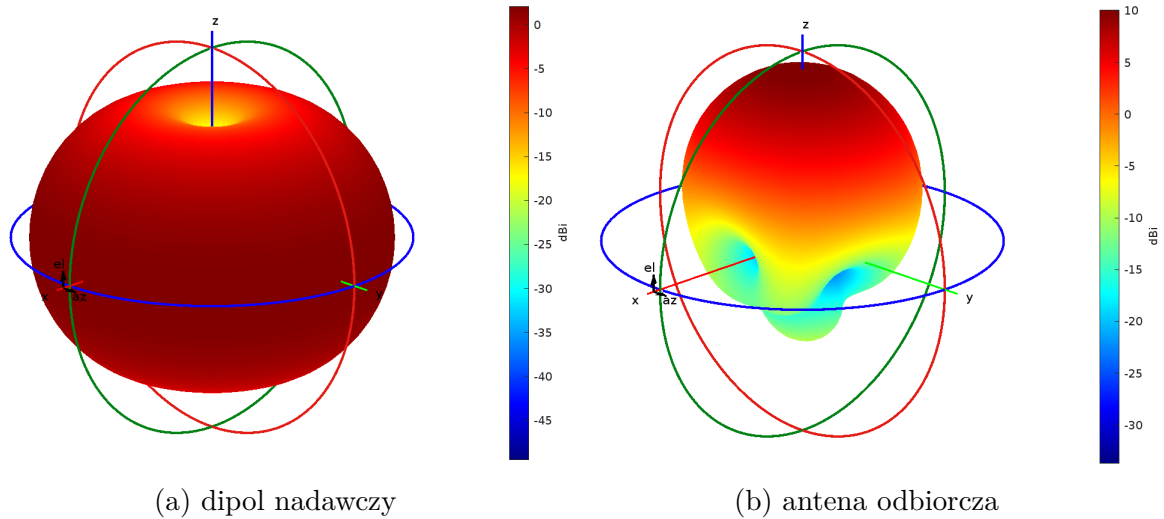
zaprojektowane systemy są w stanie przełączyć się na zapasowe środki pozycjonowania lub wygenerować ostrzeżenie dla użytkowników. Najbardziej interesujące wydają się być przypadki zakłóceń średniej mocy, ponieważ czasami mogą one być wystarczająco silne, aby wyraźnie obniżyć parametry odbiornika, ale nie na tyle, aby spowodować całkowitą utratę sygnałów satelitarnych. Podobne zachowanie możemy obserwować, kiedy obiekt wlatuje w granice strefy zakłócania.

Nowoczesne odbiorniki sygnałów nawigacji satelitarnej potrafią równolegle wykorzystywać dane z różnych systemów orbitalnych, dlatego selektywne zakłócanie jednego z nich może okazać się nieskuteczne. Komercyjnie dostępne tanie układy zagłuszające zazwyczaj posiadają oddzielne tory radiowe, a nawet anteny dopasowane do poszczególnych podpasm pracy satelitów, co jest znacznie tańsze w realizacji przy pomocy analogowych układów generowania przestrajanej fali sinusoidalnej. W proponowanym scenariuszu, posiadając tor cyfrowy, eksperymenty ukierunkowane zostały także na wykorzystanie bardziej skomplikowanych przebiegów zakłócających.

Przegląd literaturowy wykonany w poprzednich sekcjach wskazuje na różne wartości wymaganego poziomu JSR nie tylko dla wybranej techniki zakłócania, ale także dla konkretnych typów odbiorników. Dane te podsumowane zostały w tabeli 7.1 oraz uzupełnione o opracowania z poza dziedziny statków bezzałogowych. Rozrzut wyników skłania do dokładniejszego przyjrzenia się strukturze odbiornika GNSS, a także pokazuje niewystarczalność badań symulacyjnych oraz konieczność testów na rzeczywistym sprzęcie.

7.1.1 Modelowanie scenariusza zakłócania

Technologie związane z zakłócaniem sygnałów radiowych stanowią ważny element w kontekście utrzymania bezpieczeństwa i obronności, jednakże ich stosowanie jest ściśle regulowane prawnie w większości krajów. Nieautoryzowane użycie urządzeń generujących fale radiowe może naruszać przepisy telekomunikacyjne i zagrażać innym systemom łączności wykorzystywanym przez służby ratownicze oraz komercyjną flotę lotniczą. Dlatego tak

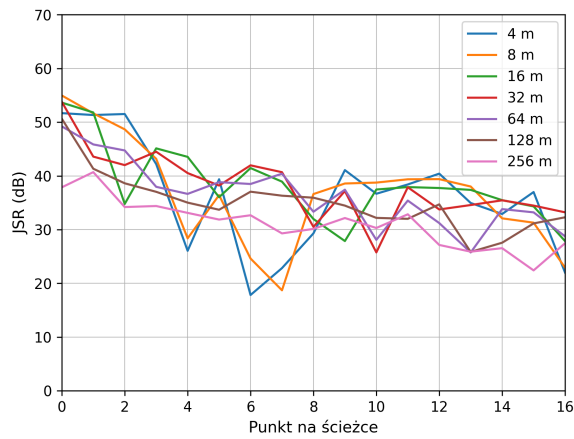


Rysunek 7.1: Charakterystyki promieniowania anten zastosowanych w symulacji zakłócania GPS L1.

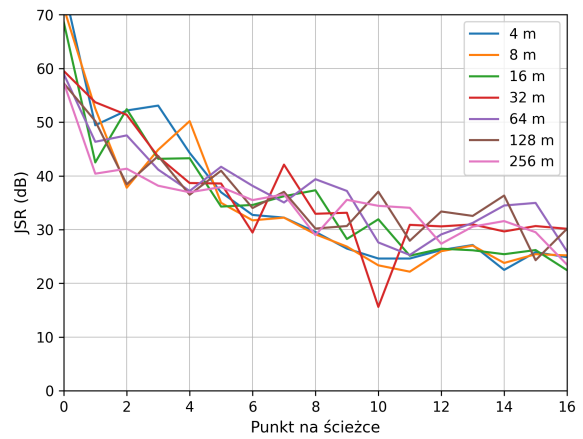
ważne jest, aby ich użycie, które staje się nieuniknione w przypadku ochrony infrastruktury krytycznej, odbywało się w sposób kontrolowany oraz przy oszacowanym poziomie ryzyka.

W eksperymencie symulacyjnym, przy podejściu statku bezzałogowego do chronionego obiektu, porównano możliwy do uzyskania stosunek JSR dla różnych wysokości lotu maszyny. Ścieżki podejścia oraz rozmieszczenie elementów są zgodne z mapą z poprzedniego rozdziału. Do tego celu zamodelowano charakterystykę wzmocnienia ceramicznej anteny GNSS, a kształt promieniowania elementu zakłócającego określono jako zgodny z klasycznym dipolem. Charakterystyki te przedstawia rysunek 7.1. Na potrzeby symulacji moc sygnału generowanego wynosiła 13 dBm, zgodnie z wcześniejszymi pomiarami prototypu, a uśredniony poziom sygnału GPS L1 przyjęto jako -130 dBm [192]. Dla każdej ścieżki podejścia zestawiono ze sobą wyniki symulacji rozmieszczenia elementu efektora wraz z detektorem, który wykazał najbardziej korzystne warunki propagacyjne w poprzednim eksperymencie. Dodatkowo przebadano wpływ umiejscowienia efektora na zerowym punkcie ścieżki, oznaczającym pozycję obiektu chronionego. Zestawienie wykresów przedstawiono na rysunku 7.2.

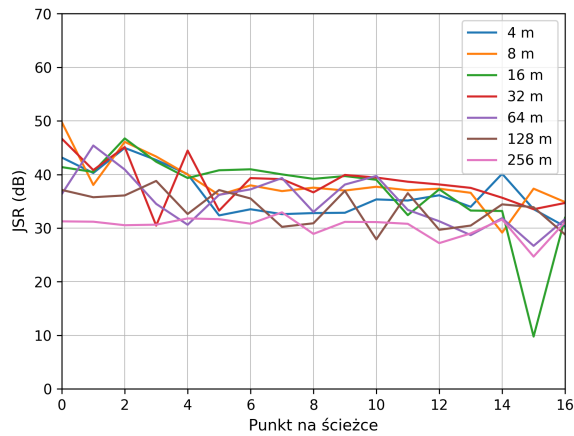
Analizując wyniki osiągalnych wartości parametru JSR w modelowanych warunkach, można przyjąć, że granica skuteczności zakłócania powinna sięgać co najmniej do trzeciego punktu na trasie przelotu drona. Zgodnie z tym założeniem opracowany prototyp może zostać użyty w środowisku rzeczywistym bez dodatkowych elementów, gdy zastosowana metoda zakłócania będzie wykazywać pożądaną skuteczność przy JSR wynoszącym 30 dB, kiedy efektor umiejscowiony będzie w pobliżu wyznaczonych lokalizacji detektorów. Alternatywnie, dla położenia nadajnika w bezpośredniej bliskości chronionego obiektu i sytuacji, w której akceptowalna jest utrata wskazania pozycji dopiero w ostatniej fazie wtargnięcia, skuteczność fali zakłócającej może objawiać się dopiero przy 50 dB wartości JSR.



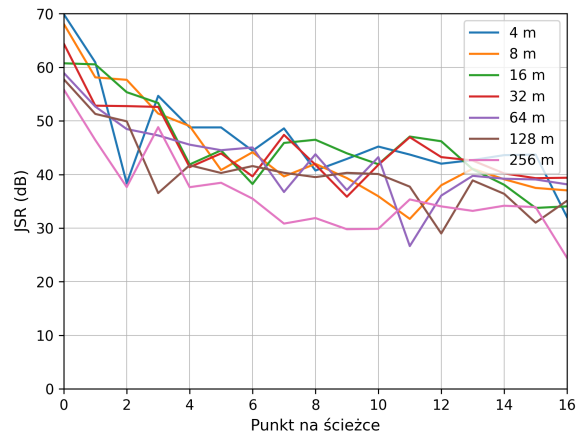
(a) *I* - pozycja "B"



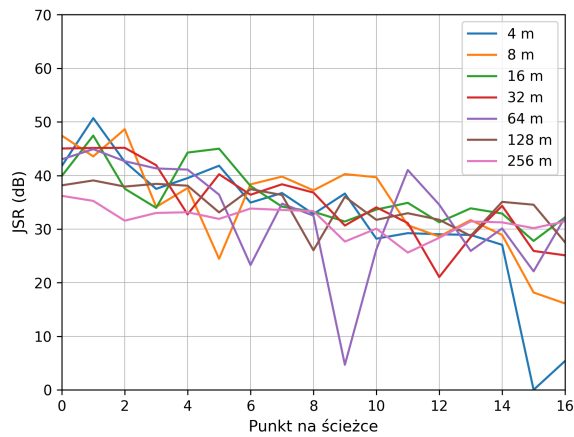
(b) *I* - pozycja "0"



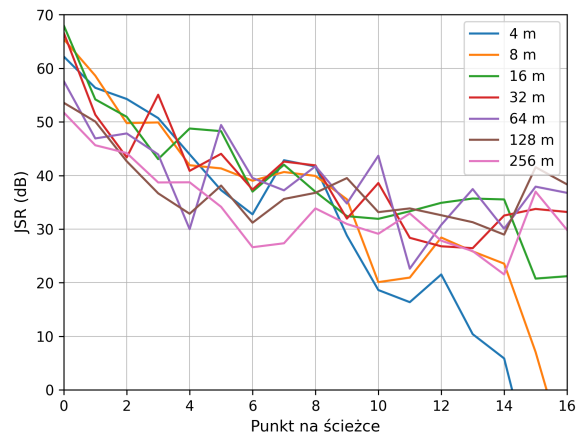
(c) *II* - pozycja "D"



(d) *II* - pozycja "0"



(e) *III* - pozycja "E"



(f) *III* - pozycja "0"

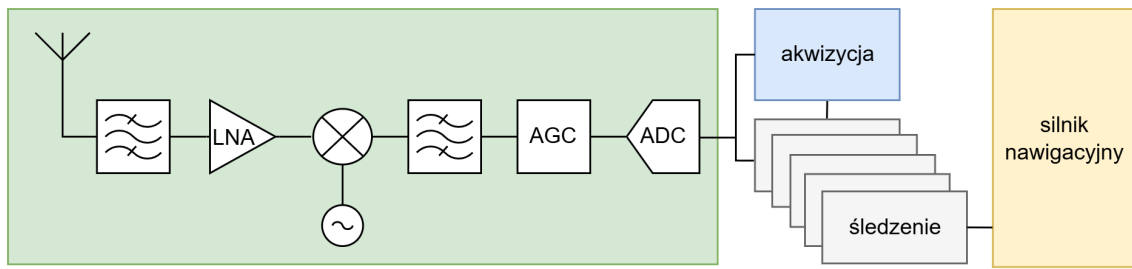
Rysunek 7.2: Wyniki symulacji metodą śledzenia promieni określające parametr JSR dla sygnału GPS L1: (a,b) dla ścieżki *I*, (c,d) dla ścieżki *II*, (e,f) dla ścieżki *III*.

7.1.2 Charakterystyka podatności odbiornika GNSS

Architektura odbiornika w urządzeniach nawigacji satelitarnej opiera się na kilku podstawowych blokach, które są odpowiedzialne za przechwytywanie, przetwarzanie i analizowanie sygnałów pochodzących z konstelacji satelitów. Schemat funkcjonalny odbiornika obejmuje antenę, końcówkę analogową, przetwornik analogowo-cyfrowy, bloki akwizycji i śledzenia, a także silnik nawigacyjny, jak pokazano na rysunku 7.3. Obecność sygnałów zakłócających ma odmienny wpływ na każdy z tych bloków [193].

Pierwszym elementem łańcucha odbiorczego jest antena, odpowiedzialna za odbiór sygnałów satelitarnych oraz ich wstępne wzmocnienie zgodnie z jej charakterystyką promieniowania. Przechwycony sygnał przechodzi przez końcówkę analogową, gdzie zazwyczaj najpierw filtr pomaga w eliminacji zakłóceń pozapasmowych, następnie LNA wzmacnia bardzo słabe sygnały pochodzące z satelitów, a konwerter częstotliwości sprowadza je na częstotliwość pośrednią lub bezpośrednio na pasmo podstawowe. Wymienione elementy charakteryzują się wysokim stopniem czułości, a w przypadku obecności silnych sygnałów zakłócających może zdarzyć się, że będą pracować poza swoim nominalnym zakresem, generując efekty nieliniowe lub przesterowania. W obu przypadkach powstaną niepożądane harmoniczne, które mogą łączyć się z sygnałem użytecznym już w pierwszej fazie przetwarzania.

Następnie sygnał formowany jest w celu uzyskania odpowiedniej dynamiki poprzez element automatycznej kontroli wzmocnienia (ang. *Automatic Gain Control*, AGC), który monitoruje poziom amplitudy wejściowej. Potem przebieg ciągły zostaje przekształcony przez przetwornik analogowo-cyfrowy na formę dyskretną, a konwersja ta obejmuje proces próbkowania i kwantyzacji. Niska moc sygnałów GNSS docierających do powierzchni ziemi sprawia, że AGC zazwyczaj jest skonfigurowane do pracy na poziomie szumu termicznego. W normalnych warunkach zmienność tego wzmocnienia jest niewielka, ponieważ średnie wahania mocy w przypadku bezpośredniej widoczności nieba są minimalne. Stała czasowa tego układu jest specyficzną cechą dla każdego odbiornika GNSS i czasem może być nawet konfigurowana przez zaawansowanego użytkownika. W niektórych przypadkach może ona wynosić około 10 ms dla obiektów stacjonarnych oraz wolno poruszających się, lub około 1-2 ms dla urządzeń takich jak samochody czy samoloty. Krótsza stała czasowa sprawia, że element AGC charakteryzuje się większą responsywnością na fluktuacje siły sygnału, lecz pętla sterowania o parametrze wynoszącym poniżej 1 ms może niekorzystnie wpływać na stabilność pracy układu. W przypadku wystąpienia zakłóceń AGC pomaga utrzymać poziom sygnału w zakresie dynamicznym i zapobiega nasyceniu przetwornika analogowo-cyfrowego, poprzez redukcję wzmocnienia w odpowiedzi na nieoczekiwany wzrost poziomu mocy. Określony charakter zmienności tego parametru jest często wykorzystywany do monitorowania pojawienia się potencjalnych zakłóceń.



Rysunek 7.3: Schemat blokowy komercyjnego odbiornika GNSS.

W kolejnym etapie cyfrowy strumień próbek trafia do modułu akwizycji, gdzie następuje próba wykrycia wszystkich satelitów znajdujących się w zasięgu odbiornika. Realizowane jest to w trybie ciągłym, gdyż satelity mogą w naturalny sposób zniknąć z pola widzenia anteny, chowając się za horyzontem, czy też ich dostępność może być ograniczona przez wysoką zabudowę miejską. Proces ten obejmuje analizę dwuwymiarowej funkcji korelacji znanej jako CAF (ang. *Cross Ambiguity Function*), mającą na celu ustalenie obecności poszczególnych sygnałów pochodzących od konkretnych satelitów, a także wstępne określenie opóźnienia fazy kodu oraz przesunięcia częstotliwości wynikającego z efektu Dopplera. Wyliczenie tych parametrów jest wymagane do inicjalizacji pętli śledzenia, niezbędnych do synchronizacji odbiornika w kolejnej fazie przetwarzania. Analiza CAF polega na porównaniu odebranego sygnału ze wszystkimi możliwymi lokalnie wygenerowanymi kodami PRN w poszukiwaniu pików korelacyjnych. Wyraźne maksimum funkcji pojawia się, gdy kod sygnału odbiorczego jest zsynchronizowany z przebiegiem lokalnym, a w przeciwnym razie funkcja zawiera jedynie szum korelacyjny. Relacja między wartością szczytową a poziomem szumu zmniejsza się wraz ze wzrostem mocy zakłóceń, co zwiększa prawdopodobieństwo fałszywego wykrycia obecności sygnału oraz dostarczenia błędnych szacunków wpływu efektu Dopplera i opóźnienia kodu.

Odnalezione w poprzednim kroku sygnały satelitów trafiają na indywidualne jednostki śledzące, których głównym zadaniem jest dalsze precyzowanie parametrów związanych z lokalnym przesunięciem fazy kodu oraz częstotliwości. Odbywa się to za pomocą pętli synchronizacji fazowej, która koncentruje się na utrzymaniu synchronizacji z sygnałem nośnym, oraz pętli synchronizacji opóźnienia, która pomaga utrzymać synchronizację z fazą kodu PRN danego satelity. Stopnie śledzące wykorzystują architekturę zamkniętej pętli sterowania i opierają swoje działanie na korelatorach sygnałów, dyskryminatorach oraz filtrach pętlowych. W standardowych odbiornikach trzy korelatory: wczesny, właściwy i późny, używane są do śledzenia kodu, a jeden korelator wystarcza do śledzenia nośnej. Dyskryminatory natomiast wykorzystują sygnały wyjściowe korelatorów do określenia błędów między szacowanymi a rzeczywistymi parametrami sygnału. W warunkach normalnej pracy zadaniem pętli jest sprowadzenie wartości wyjściowych z tego elementu w okolice zera, toteż obserwacja wzrostu poziomu szumu, który prowadzi do ogólnego zwiększenia wariancji w tym przebiegu, może być wykorzystana do oceny obecności zakłóceń. Ma to bezpośredni

wpływ na jakość danych wypracowywanych przez moduł śledzący, powodując zwiększone odchylenia pomiarowe i możliwe błędy dekodowania komunikatu nawigacyjnego.

Po akwizycji i śledzeniu sygnałów GNSS silnik nawigacyjny wykorzystuje wypracowane wartości do obliczenia lokalizacji odbiornika. Określane jest to za pomocą triangulacji położenia odbiornika w odniesieniu do śledzonych pozycji satelitów. Jeśli zakłócony sygnał może być nadal przetwarzany zarówno przez etapy akwizycji, jak i śledzenia, moduł będzie w stanie oszacować pozycje, jednak wyliczenie będzie oparte na zniekształconych pseudo-odległościach. Rzeczywisty błąd silnie zależy od konkretnego algorytmu pozycjonowania, a sygnał zakłócający, w zależności od wartości parametru JSR, pogarsza wskazanie lub powoduje całkowitą utratę funkcjonalności [194].

Monitorowanie pewnego zbioru parametrów, będących wynikiem przetwarzania sygnałów na różnych etapach łańcucha odbiorczego, może także posłużyć do wykrywania obecności zakłóceń. Techniki te obejmują na przykład obserwację charakteru odpowiedzi pętli AGC, która w warunkach pracy normalnej nie powinna zawierać gwałtownych skoków wzmocnienia. Na tym etapie przetwarzania możliwe jest również analizowanie średniej energii próbek w danym oknie czasowym oraz analiza funkcji gęstości prawdopodobieństwa, polegająca na porównaniu rozkładu z tym uzyskanym w sytuacji bez zakłóceń. W warunkach normalnych można modelować ten proces zgodnie z krzywą Gaussa o zerowej wartości średniej, podczas gdy zakłócenia powodują znaczne odchylenia od tego wzorca, a miarą tego zjawiska może być kurtoza przebiegu. Do najpopularniejszych technik należy obserwacja współczynnika C/N_0 , który w obecności zakłóceń ulega znacznemu pogorszeniu z powodu wzrostu poziomu szumu w odniesieniu do sygnałów właściwych. Obserwacja wymienionych współczynników może być dodatkowo skumulowana i zastosowana do reprezentacji cech wejściowych dla metod uczenia maszynowego, co zostało przeanalizowane w [195].

Zdolność odbiornika do przywrócenia prawidłowego stanu podczas zakłóceń poprzez zminimalizowanie lub wyeliminowanie wpływu niepożądanych sygnałów może być realizowana na kilka sposobów. Pierwszym z nich jest maskowanie impulsowe w dziedzinie czasu (ang. *Pulse Blanking*), które polega na zerowaniu zestawu próbek, w których wystąpiło podejrzenie zniekształcenia. Proces ten często sprzężony jest z analizą odpowiedzi AGC, zależy od stałej czasowej pętli regulacji i wykazuje dużą skuteczność w eliminacji krótkotrwałych, zazwyczaj nieintencjonalnych zakłóceń. Metody przeciwdziałania w dziedzinie częstotliwości są natomiast powszechnie stosowane w przypadku zakłóceń wąskopasmowych oraz ciągłych. Jedną z technik w tej kategorii jest estymacja widma poprzez zastosowanie DFT i filtrację niepożądanych częstotliwości, co w przypadku tego rodzaju zakłóceń ma niewielki wpływ na sygnał właściwy. Po tym procesie reprezentacja czasowa jest odtwarzana poprzez zastosowanie transformacji odwrotnej. Metoda ta wykazuje największą skuteczność, gdy charakterystyka sygnału zakłócającego pozostaje stała w czasie. W przeciwnym razie, jak na przykład w przypadku zakłóceń przestrajanych, występuje

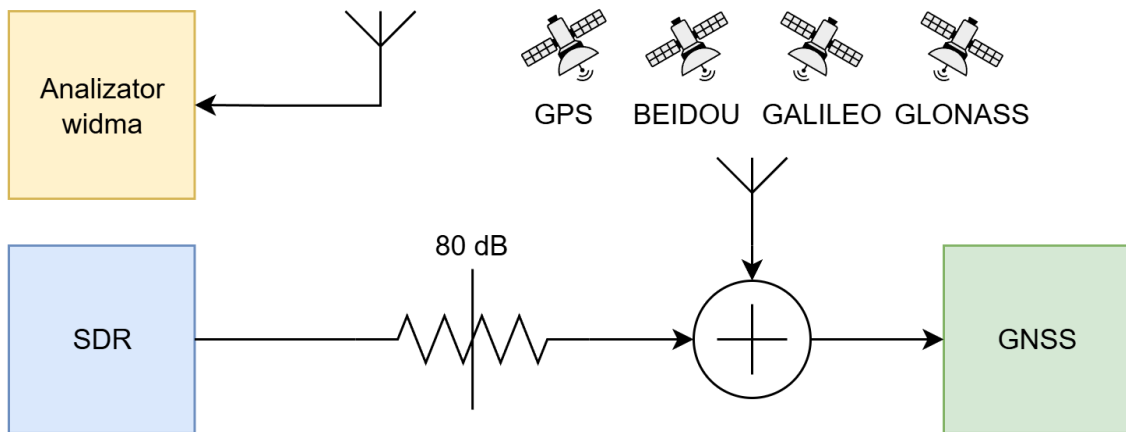
konieczność stosowania metod adaptacyjnych polegających na wprowadzeniu filtrowania podczas obserwacji spektrum w niewielkim przedziale czasowym. Alternatywnie, możliwe jest także stosowanie rozszerzonej koncepcji filtra wycinającego (ang. *Notch Filter*) z dodatkową jednostką adaptacyjną, która w sposób ciągły śledzi i tłumi zmienne w czasie zakłócenia [194].

Poza rozwiązaniami operującymi wyłącznie na pojedynczym sygnale, szereg nowych możliwości otwierają koncepcje filtrowania przestrzennego oraz anteny ze sterowaną wiązką, znane z systemów radarowych. Metoda ta polega na wykorzystaniu układu anten rozmieszczonych w określonej konfiguracji geometrycznej, która zapewnia dostarczenie opóźnionej w czasie wersji odbieranego sygnału przy zwiększonej różnorodności przestrzennej. Regulacja fazy oraz amplitudy sygnałów odbieranych przez poszczególne elementy antenowe w układzie powoduje wytworzenie punktu zerowego (ang. *null steering*) w skumulowanej charakterystyce promieniowania. Działanie to skutkuje tłumieniem sygnałów docierających do układu z określonych kierunków, przy zachowaniu czułości w innych kierunkach. Rozwiązanie to jest niezwykle skuteczne w tłumieniu intencjonalnych zakłóceń, jednakże poza wymogiem stosowania zaawansowanych technik przetwarzania, konieczne jest odpowiednie rozmieszczenie przestrzenne elementów antenowych, co zwiększa rozmiar rozwiązania. Dodatkowo, koszt takiego urządzenia, masa oraz zapotrzebowanie energetyczne sprawiają, iż nie jest ono powszechnie stosowane w komercyjnych statkach bezzałogowych.

Chociaż metoda adaptacyjnego formowania wiązki jest jednym z najskuteczniejszych sposobów poprawy odporności odbiornika na zakłócenia, to gdy liczba źródeł zakłóceń jest większa lub równa liczbie układów antenowych, osiągnięcie pożądanego efektu jest ograniczone. Dlatego też rozmieszczenie wielu rozproszonych źródeł sygnałów jest skutecznym sposobem, nawet w zestawieniu z tą techniką. Sposób rozmieszczenia źródeł będzie miał bezpośredni wpływ na rozkład mocy zakłóceń w danym obszarze i ostatecznie wpłynie na skuteczność systemu przeciwdziałania. Obecne badania nad rozmieszczeniem źródeł zakłóceń opierają się głównie na analizie mocy oraz na geometrycznych modelach źródeł promieniowania. Sprowadza to zadanie do problemu optymalizacyjnego, który może być rozwiązany na przykład przez algorytmy genetyczne [196].

7.1.3 Eksperymenty

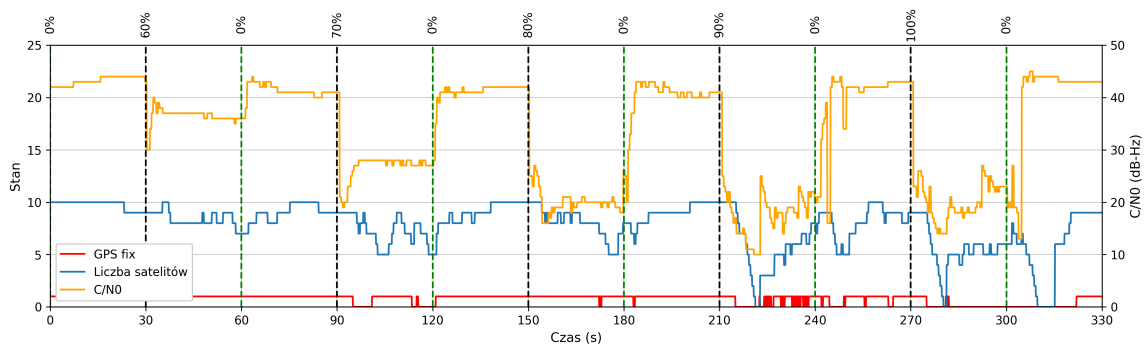
Podstawą zbudowanego zestawu eksperymentalnego jest odbiornik u-blox dziewiątej generacji osadzony na zestawie ewaluacyjnym EVK-F9P [197]. Producent w tym przypadku zapewnia oprogramowanie, które pozwala monitorować poszczególne parametry sygnałów satelitarnych, w przeciwieństwie do zwykłego zestawu dronowego, w którym dostępność informacji o jakości GNSS jest bardzo ograniczona. Stanowisko pomiarowe przedstawione jest na schemacie 7.4. Zdecydowano się na zastosowanie metody, która wykorzystuje rzeczywiste sygnały nawigacyjne, sumowane w torze analogowym z transmi-



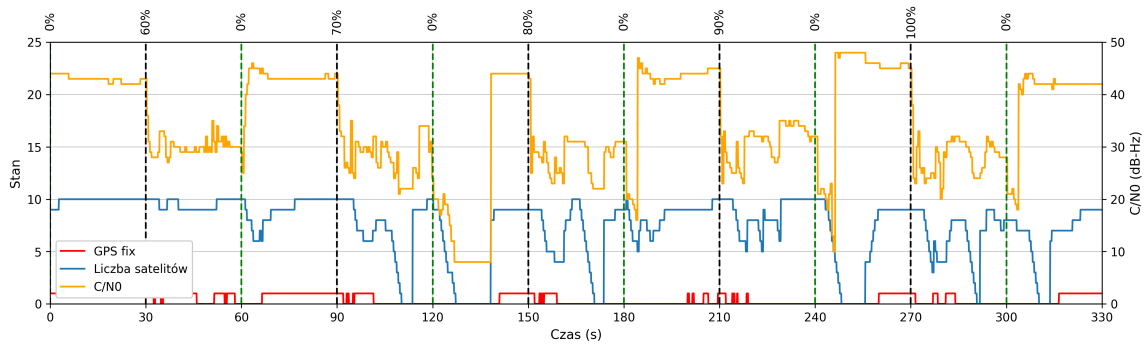
Rysunek 7.4: Schemat blokowy stanowiska pomiarowego dla zakłócania sygnałów GNSS.

sjami zakłócającymi. Wszystkie eksperymenty przebiegają według scenariusza, w którym moc sygnału zakłócającego zmienia się co 30 s, a zakres czasu obserwowanego na przebiegach zawiera fragmenty z istotnymi reakcjami odbiornika. Moc nadajnika, przedstawiona w procentach pełnego wystawienia prototypu efektora, jest podnoszona krokowo o 10% do uzyskania 100% wystawienia, co przeplatane jest fazami wyciszenia. Dzięki temu odbiornik ma szansę na ponowną synchronizację z sygnałem satelitów, a każda kolejna próba zakłócenia rozpoczyna się od fazy śledzenia, a nie od wyszukiwania. Sprawia to, że w każdym kolejnym kroku odbiornik ma porównywalne warunki początkowe. Do obserwacji jego zachowania wybrano trzy główne parametry, w tym współczynnik C/N_0 , liczbę satelitów zatrzaśniętych w fazie śledzenia oraz pojedynczy wyznacznik wskazujący w binarny sposób możliwość wyznaczenia pozycji w danej chwili czasu (ang. *fix*).

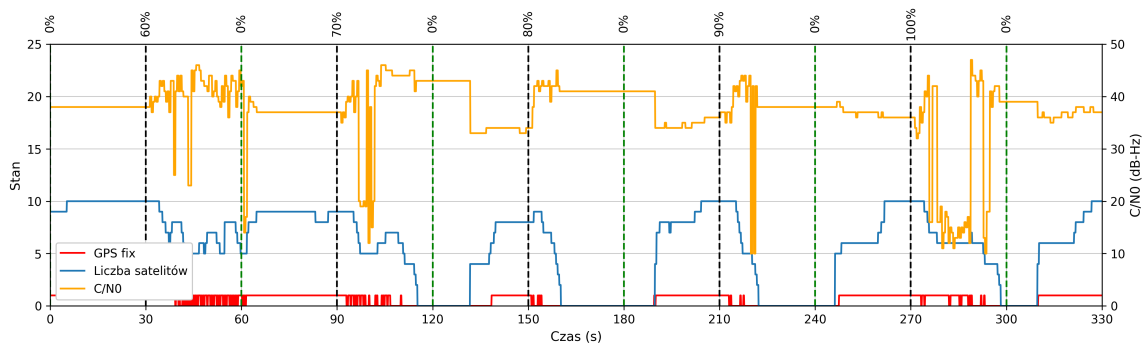
W pierwszym eksperymencie porównano możliwości prototypu efektora, badając wpływ podstawowych technik zakłócania na odbiornik operujący tylko w konstelacji GPS, co jest częstym scenariuszem w wielu opracowaniach. Nadajnik skonfigurowano na częstotliwość środkową wynoszącą 1575,42 MHz z pasmem 20 MHz, a wystawienie zmieniane od 60% do 100% odpowiadało mocy na wyjściu efektora od -8 dBm do 13 dBm. Wartość tłumienia na stanowisku testowym ustawiono na 80 dB, co przy założeniu mocy sygnału GPS na poziomie -130 dBm, jak w symulacjach, powinno odpowiadać zmienności JSR od 42 dB do 63 dB. Wyniki pomiarów dla trzech zastosowanych metod pokazane są na wykresie 7.5. Dla zakłócania pojedynczym tonem, zgodnym z częstotliwością środkową pasma GPS L1, mimo widocznego systematycznego spadku zarówno liczby satelitów, jak i współczynnika C/N_0 , pełna utrata wskazania pozycji nastąpiła dopiero przy maksymalnej mocy nadajnika. Warto w tym miejscu zauważyć, iż współczynnik ten bardzo dynamicznie reaguje na pojawienie się zakłóceń oraz na ich zanik. W tym przypadku odbiornik, mimo ciągłego występowania zakłócenia, jest też w stanie odpracować po chwili zarówno poziom C/N_0 , jak i liczbę satelitów do pewnego stopnia, co może świadczyć o uruchomieniu algorytmów przeciwdziałania. Dla techniki świadomej, w której zastosowano zmodulowany



(a) ton pojedynczy



(b) modulacja BPSK



(c) fala przestrajana

Rysunek 7.5: Wpływ różnych fal zakłócających na parametry odbiornika podczas zakłócania konstelacji GPS L1.

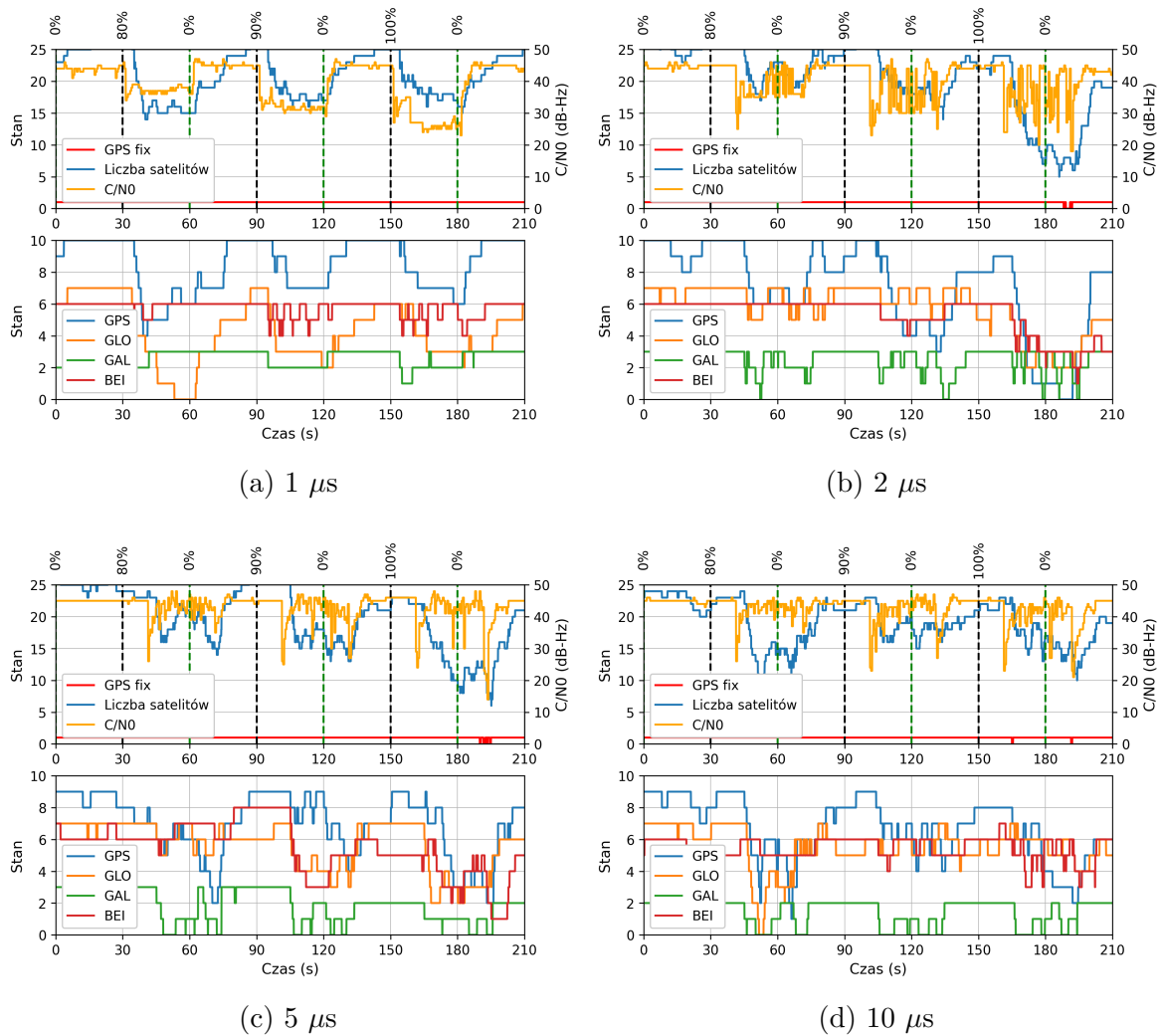
sygnał BPSK z częstotliwością 1,023 MHz, spadek współczynnika C/N_0 nie pogłębia się wraz ze wzrostem mocy tak znacząco jak w przypadku zakłóceń pojedynczym tonem, ma jednak znacznie większą zmienność, a reakcja odbiornika jest tu widoczna już przy wystawieniu wynoszącym 60%. Dla zakłóceń przestrajanych jednokierunkowych o zakresie zmienności 20 MHz wokół częstotliwości środkowej GPS L1 i czasie przemiatania równym $10 \mu s$ pierwsze efekty można zauważyć także przy wystawieniu równym 60%. W tym przypadku interesujący jest fakt, iż układ traci i odzyskuje możliwość wskazywania pozycji praktycznie z próbki na próbkę, a szacowanie współczynnika C/N_0 przez odbiornik wydaje się mocno zaburzone.

Tabela 7.2: Systemy nawigacji satelitarnej wykorzystywane w popularnych modelach statków bezzałogowych.

Producent	Model	Zakres	GPS	GLONASS	GALILEO	BeiDou
Autel	EVO Max 4T	L1	TAK	TAK	TAK	TAK
DJI	MAVIC 4	L1	TAK	NIE	TAK	TAK
DJI	INSPIRE	L1	TAK	NIE	TAK	TAK
DJI	MINI	L1	TAK	NIE	TAK	NIE
FIMI	X8 Mini	L1	TAK	TAK	NIE	TAK
Husban	ZINO MINI	L1	TAK	TAK	NIE	NIE
Parrot	Anafi	L1	TAK	TAK	TAK	NIE
Skydio	X10	L1	TAK	TAK	TAK	TAK

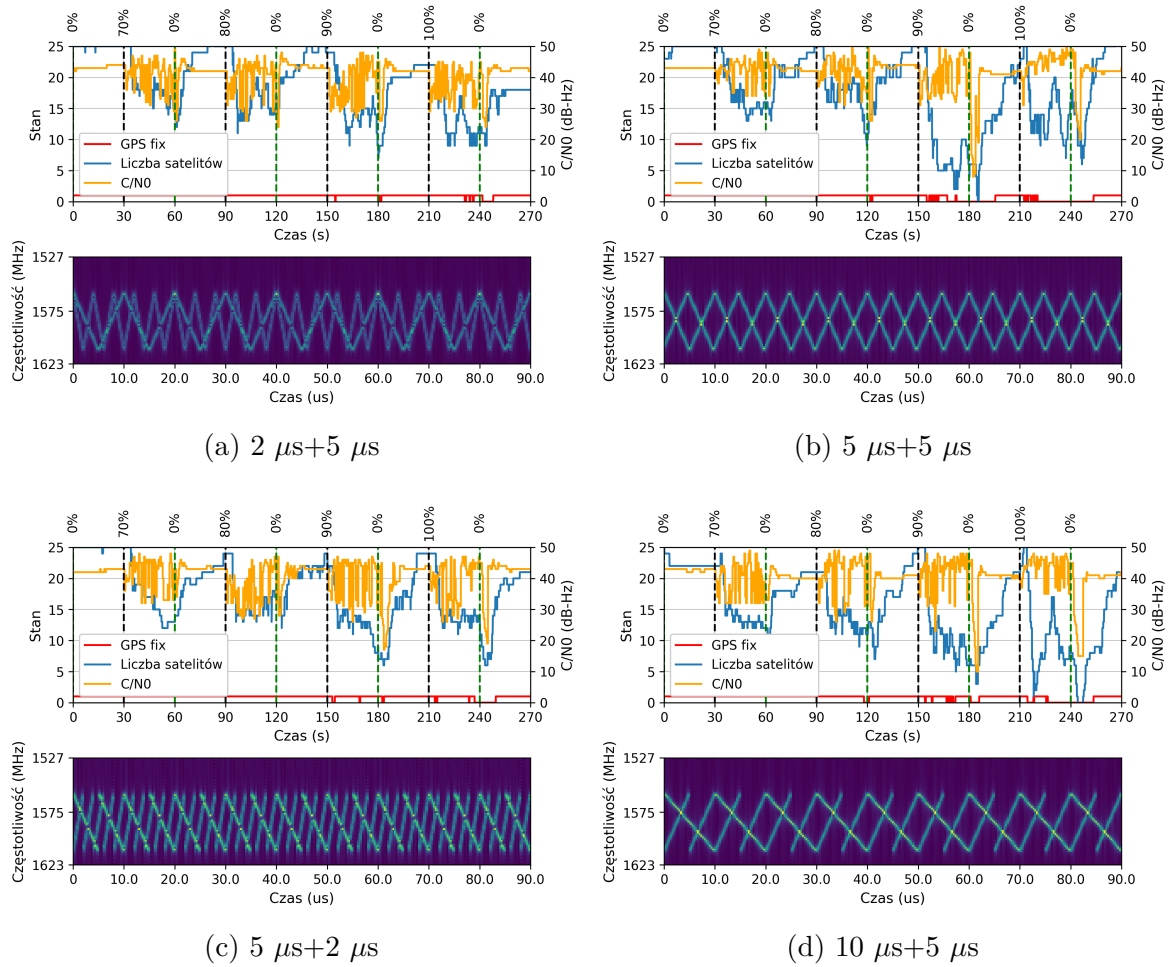
W odbiornikach GNSS starszej generacji określenie dwupasmowy wiązało się najczęściej z obsługą zarówno konstelacji GPS L1, jak i GLONASS L1. Współcześnie taka funkcjonalność jest standardem, a nowoczesny odbiornik jednopasmowy zazwyczaj do wyznaczania pozycji potrafi zastosować już trzy niezależne systemy: GPS L1, GLONASS L1 i BeiDou B1. Najnowsza generacja odbiorników z profesjonalnej kategorii, w tym badany u-blox F9, obsługuje również GALILEO E1. Przegląd systemów stosowanych w konkretnych modelach bezzałogowych statków powietrznych podsumowano w tabeli 7.2. Integracja odbiorników zdolnych do obsługi wszystkich czterech systemów nawigacji w dronach obecnych na rynku komercyjnym stawia wymaganie, aby układ zakłócający posiadał zdolność operacji w zakresie częstotliwości od 1559 MHz do 1610 MHz.

W eksperymencie drugim układ stanowiska pozostał niezmieniony, ale w odbiorniku aktywowana została obsługa wszystkich dostępnych konstelacji GNSS. Tym razem nadajnik ustawiono jednak na częstotliwość środkową 1584,5 MHz z pasmem 51 MHz. Celem badania była obserwacja wpływu sinusoidalnej fali przestrajanej na wskazania odbiornika z podziałem na konkretne systemy nawigacji, w odniesieniu do czasu powtarzania przebiegu. Zestawienie wyników dla czterech różnych okresów przedstawiają wykresy na rysunku 7.6. Wytrącanie wielokanałowego odbiornika z fazy wskazywania pozycji udało się jedynie dla najwyższego ustawienia mocy oferowanej przez efektor, a proces ten był najbardziej skuteczny w przypadku okresu 2 μ s i 5 μ s. Dodatkową obserwacją jest tu odmienny wpływ poszczególnych czasów przestrajania na dane systemy nawigacyjne. Choć podczas badania liczba satelitów Galileo była wyraźnie najmniejsza, to najbardziej dynamiczny spadek ich udziału w obliczeniach pozycji widać dla okresów przemiatania 5 μ s i 10 μ s. Dla systemu BeiDou i czasu 5 μ s spadek liczby satelitów rozpoczyna się już od 80% wysterowania nadajnika i w próbie tej odnotowano najbardziej dynamiczną reakcję odbiornika na zakłócenia. Dla konstelacji GPS reakcje na zakłócanie z okresem 2 μ s są najbardziej dynamiczne i przy wysterowaniu 100% liczba satelitów spada najniżej. Finalnie dla GLONASS sytuacja wygląda niejednoznacznie, niezależnie od czasu przestrajania.



Rysunek 7.6: Parametry odbiornika podczas zakłócania GNSS sinusoidalnym sygnałem przestrajającym w zakresie 1559 MHz do 1610 MHz z różnym czasem powtarzania.

Aby w pełni przetestować możliwości odbiornika, w ostatniej serii testów nadajnik ustawiono na częstotliwość środkową 1575,42 MHz z pasmem 96 MHz, a przesunięcie fali na środek zakresu 1559-1610 MHz wykonano cyfrowo przy generacji próbek w środowisku Matlab. Bazując na obserwacjach z poprzedniego eksperymentu połączono ze sobą dwie fale sinusoidalne w kilku kombinacjach. Najciekawsze z nich przedstawia zestawienie na rysunku 7.7. Połączenie fal o czasie przemiatania $2 \mu\text{s}$ i $5 \mu\text{s}$ dało zdecydowanie lepsze rezultaty niż w przypadku fali pojedynczej. Pierwsze utraty sygnału widać w tym przypadku przy 90% wysterowania, a większy wpływ na wskazanie pozycji ma fala z przemiataniem jednokierunkowym niż ta z trójkątnym. Najskuteczniejszym w tej serii przebiegiem okazało się natomiast zestawienie przeciwnieprzestrajanych fal o czasie powtarzania $10 \mu\text{s}$ i $5 \mu\text{s}$. Spadek liczby satelitów był tu wyraźnie pogłębiany z każdym krokiem, a pierwsze straty wskazania pozycji widać przy 80% wysterowania. Biorąc pod uwagę założenia symulacyjne, przekłada się to na co najmniej 58 dB stosunku JSR, który wymagany jest



Rysunek 7.7: Parametry odbiornika podczas zakłócania GNSS kombinowanym sygnałem przestrajającym.

do zakłócenia odbiornika. Powoduje to, iż efektor bez dodatkowych wzmacniaczy mocy, umieszczony w bezpośredniej bliskości elementu krytycznego, jest w stanie zakłócić pracę drona przebywającego nad celem do wysokości około 64 m. Przy dolocie natomiast na 8 metrach wysokości zasięg działania efektora wydłuża się do około 130 m.

7.2 Sygnały kierowania i kontroli

Sygnały kierowania i kontroli wykorzystywane są do przesyłania komend sterujących w kierunku od operatora do statku bezzałogowego, a także do transmisji obrazu oraz danych telemetrycznych w stronę przeciwną. Zagłuszanie tych sygnałów jest bardziej skomplikowane niż w przypadku systemów nawigacji satelitarnej, gdyż ten rodzaj łączności charakteryzuje się wyższymi poziomami mocy nadawanej oraz specjalnymi algorytmami ograniczającymi skuteczność tego procesu. Emisja z satelitów ma z góry określone parametry, takie jak częstotliwość środkowa i rodzaj modulacji, a procesy związane z przetwarzaniem tych danych są dostępne publicznie. W przypadku sygnałów dronowych natomiast

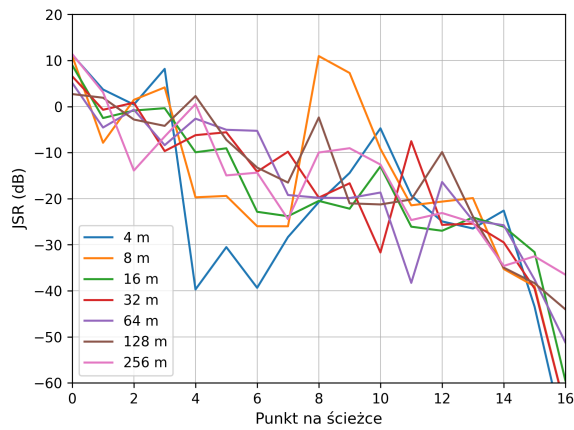
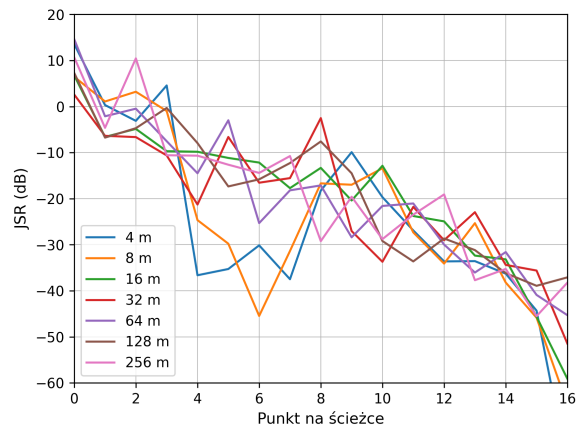
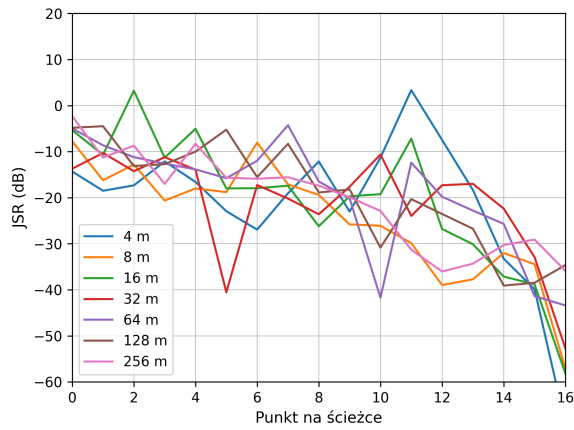
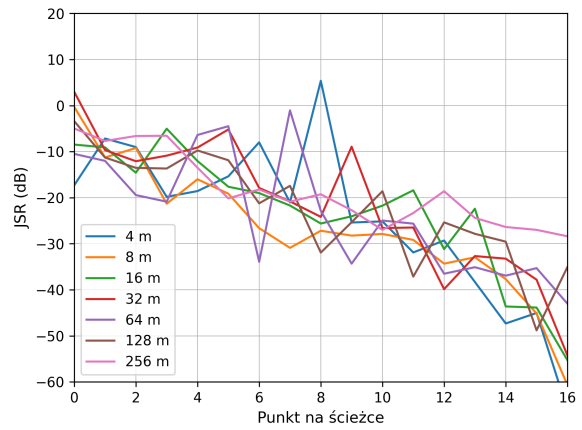
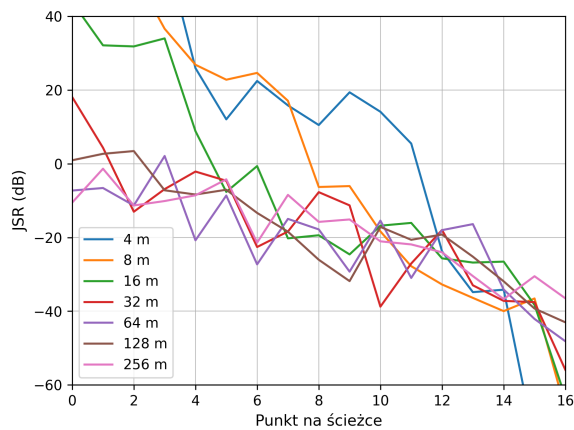
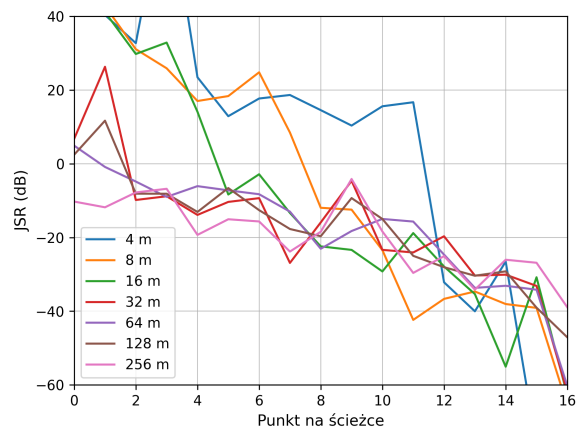
można mówić o empirycznym rozpoznaniu charakteru transmisji, gdyż jest to zazwyczaj chroniona własność intelektualna każdego producenta. Dodatkową trudność i różnice w podejściu do zakłócania stanowi powszechnie stosowana technika przeskoków częstotliwości, która powoduje rozproszenie widma na dużą szerokość oraz stosowanie kodów korekcyjnych, uodporniających przesył na pojedyncze błędy bitowe.

Następstwa zagłuszania łączności uzależnione są od skali i rodzaju ich występowania. W przypadku zakłóceń chwilowych, które mogą wystąpić także z powodu interferencji z innymi urządzeniami, statek bezzałogowy może wykazywać nieprzewidywalne zachowanie w locie, ponieważ komunikaty będą docierały do niego z opóźnieniem bądź fragmentarycznie. Natomiast w przypadku całkowitego zaniku łączności dron może przejść w tryb awaryjny i podjąć próbę powrotu do bazy, jeśli dostępny będzie sygnał nawigacji satelitarnej. Zamiast tego, w obliczu braku sygnałów GNSS, maszyna może pozostawać w zawisie do momentu wyczerpania baterii.

7.2.1 Modelowanie scenariusza zakłócania

W eksperymencie symulacyjnym dotyczącym zakłóceń sygnałów GNSS, przy podejściu statku bezzałogowego do chronionego obiektu, porównano możliwy do uzyskania stosunek JSR dla różnych wysokości lotu maszyny. W przypadku sygnałów kierowania i kontroli przyjęto ten sam scenariusz, ale dodatkowym elementem jest tu układ nadawczy operatora drona umieszczony w ostatnim punkcie ścieżki. Aby w danej pozycji obiektu na ścieżce wyznaczyć współczynnik JSR, przeprowadzono symulacje poziomu sygnału emitowanego z najbliższego efektora, co zostało zestawione z wartościami generowanymi przez aparaturę sterującą. Przyjęto tutaj moc 20 dBm dla 2,4 GHz oraz 14 dBm dla 5,8 GHz, przy dostępnej dla prototypu efektora mocy odpowiednio dla tych częstotliwości 4 dBm oraz -3 dBm. Zestawienie wykresów przedstawiono na rysunku 7.8.

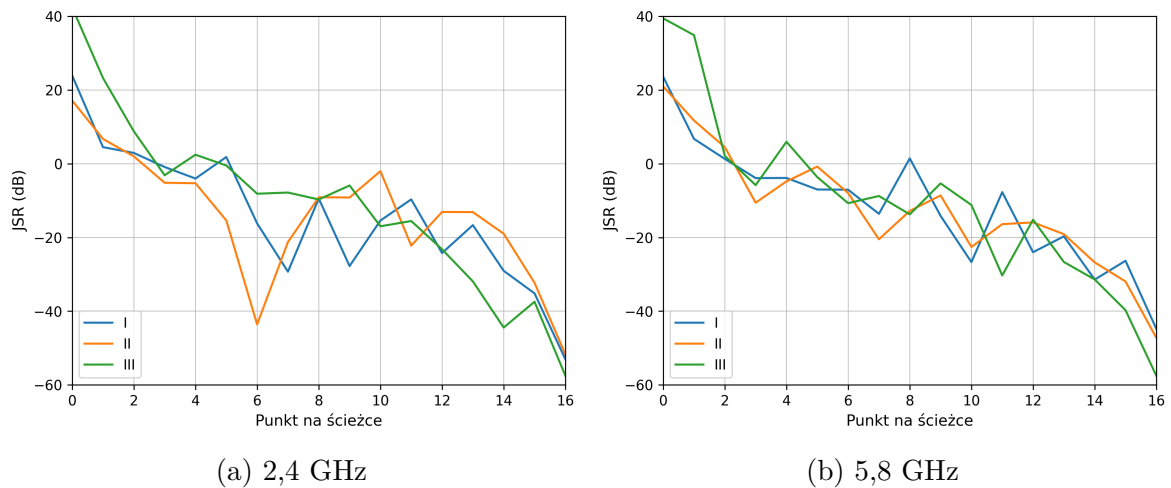
Prototyp efektora oferuje znacznie mniejszą moc wyjściową dla częstotliwości 2,4 GHz w odniesieniu do 1,5 GHz, a poziom sygnałów generowanych przez aparaturę sterującą jest dużo wyższy niż w przypadku GNSS. Obie te charakterystyki niekorzystnie wpływają na możliwe do uzyskania stosunki JSR w przypadku próby zagłuszania sygnałów sterujących bezzałogowym statkiem powietrznym. Dla podejścia pierwszego efektor umieszczony jest najbliżej chronionego miejsca, którego odległość wynosi 100 m, podczas gdy operator znajduje się 2600 m dalej. Dodatni współczynnik JSR dla obu częstotliwości możliwy jest do uzyskania tylko w punkcie pomiarowym położonym bezpośrednio nad chronioną stacją. Dla drugiego podejścia, gdzie efektor umieszczony jest 400 m od celu, a odległość operatora wynosi 1200 m, dodatni współczynnik praktycznie nie jest osiągalny z uwagi na brak przeszkód osłabiających właściwy sygnał sterujący. Dla podejścia trzeciego, gdzie efektor również znajduje się 400 m od celu, odległość operatora wynosi 3000 m. W tym przypadku znaczne osłabienie toru bezpośredniej widoczności pomiędzy dronem a operatorem na


(a) *I* - pozycja "B" 2,4 GHz

(b) *I* - pozycja "B" 5,8 GHz

(c) *II* - pozycja "D" 2,4 GHz

(d) *II* - pozycja "D" 5,8 GHz

(e) *III* - pozycja "E" 2,4 GHz

(f) *III* - pozycja "E" 5,8 GHz

Rysunek 7.8: Wyniki symulacji metodą śledzenia promieni określające parametr JSR dla sygnałów sterujących: (a,b) dla ścieżki *I*, (c,d) dla ścieżki *II*, (e,f) dla ścieżki *III*.

wysokościach do 16 m poprawia warunki pracy prototypu efektora.

Przyjmując wysokość podejścia na 32 m za taką, która zapewnia dobre warunki propagacyjne dla komunikacji pomiędzy statkiem bezzałogowym a operatorem, w kolejnym



Rysunek 7.9: Wyniki symulacji metodą śledzenia promieni określające parametr JSR dla sygnałów kierowania i kontroli dla drona operującego na wysokości 32 m.

eksperymentie efektor został umieszczony w bezpośredniej bliskości chronionego obszaru. Przeprowadzone symulacje wskazują, że dodatnia wartość JSR dla tej konfiguracji efektorów może być zachowana na dwóch pierwszych punktach ścieżki w dolocie drona do celu, co zaprezentowano na rysunku 7.9.

7.2.2 Charakterystyka podatności odbiornika OFDM

Technologia OFDM jest szeroko stosowana w nowoczesnych systemach komunikacyjnych ze względu na jej odporność na zjawiska wielodrogowości i wysoką wydajność widmową. Jednakże wymagania dotyczące ścisłej synchronizacji i wrażliwość na szacowanie kanału zwiększają podatność OFDM na ataki zakłócające.

Szerokopasmowe zakłócanie zaporowe jest podstawowym i najprostszym ze wszystkich ataków, nie wymagającym dodatkowych informacji o celu i jest dobrą strategią zakłócania w przypadku braku jakiegokolwiek wiedzy o sygnale docelowym. Ten typ zakłócania jest często traktowany jako punkt odniesienia do analizy także innych technik przeciwdziałania. W przypadku transmisji sygnałów z platform bezzałogowych, podbicie poziomu szumu, a co za tym idzie, zmniejszenie odbieranego SNR, musi nastąpić w całym paśmie ISM, z uwagi na zastosowane techniki przeskoków częstotliwości dla kanału sterowania. Natomiast dla ścieżki transmisji obrazu w dronach stosowane jest podejście adaptacyjne, gdzie w sposób automatyczny dobierany jest fragment widma o najniższym poziomie szumu. Wymagania dotyczące niezbędnego stosunku sygnału do szumu dla technologii OFDM są zróżnicowane w odniesieniu do poszczególnych zastosowań, ale generalnie dąży się do uzyskania wysokich wartości w celu zapewnienia dobrej wydajności i niezawodności. Duże znaczenie ma tu także zastosowana modulacja podnośnych, która ustali pewien poziom tych wymagań. Dokładne wartości są indywidualną cechą odbiornika, ale jak wskazuje badanie, mogą

one wynosić na przykład 3,63 dB dla BPSK, 8,40 dB dla QPSK czy nawet 21,63 dB dla 64QAM [198].

Zakłócanie przestrajane również jest skuteczne w przypadku sygnałów OFDM, osiągając lepsze wyniki w stosunku do techniki zaporowej dzięki niższej wartości stosunku mocy szczytowej do średniej [199]. Podobnie jak w przypadku oddziaływania na sygnały nawigacji satelitarnej, ma tu znaczenie zarówno czas, jak i pasmo przestrajania. Na przykład dla JSR poniżej -26 dB i niezależnie od czasu przestrajania osiągalna szybkość transmisji dla standardu 802.11n jest maksymalna, co oznacza, że ta technika nie ma wpływu na wydajność systemu. Jednak dla JSR wynoszącego -20 dB, a więc w momencie kiedy sygnał zakłócający silniejszy jest o 6 dB, mogą wystąpić różne zachowania w zależności od okresu sygnału zakłócającego [200].

Istnieje także szereg selektywnych sposobów zakłócania, które precyzyjnie trafiają w krytyczne składowe transmisji używającej OFDM. Jak wskazano wcześniej, niektóre podnośne w OFDM zawierające sygnały pilotów, które są istotną częścią tego systemu, ponieważ są wykorzystywane do śledzenia charakterystyki kanału oraz do poprawy dokładności synchronizacji. Próba zakłócania tylko sygnałów pilotów, wprawdzie daje poprawę skuteczności rzędu 2 dB w stosunku do techniki zaporowej, ale wymaga znajomości ich rozmieszczenia i odpowiedniej synchronizacji nadajnika. Rozszerzeniem tej metody jest zerowanie pilotów, które zwiększa ten stosunek do 7,5 dB, ale tu konieczne jest wręcz posiadanie dokładnej wiedzy o ich strukturze [201].

W systemach OFDM niedoskonałość synchronizacji częstotliwości w dużo większym stopniu oddziałuje na poprawność transmisji niż błędy synchronizacji czasowej. Niedoskonałości sprzętowe oscylatorów czy wpływ warunków środowiskowych powodują, że mimo ustawienia wspólnej częstotliwości, układy te wymagają dostrojenia w czasie rzeczywistym. Proces estymacji przesunięcia częstotliwości przebiega zazwyczaj w odbiorniku zaraz po detekcji preambuły. Przy słabej synchronizacji częstotliwościowej wydajność OFDM ulega znacznemu pogorszeniu, ponieważ mogą wystąpić naruszenia ortogonalności podnośnych i błędy estymacji kanału. Sygnał zakłócający więc, wygenerowany we właściwym momencie, może pozwolić na ograniczenie transmisji stacji zakłóceń nawet do 1% czasu trwania ramki właściwej [202]. W tym przypadku wymagana jest jednak znajomość położenia fragmentu odpowiedzialnego za proces korekcji przesunięcia w ramce oraz bardzo szybka reakcja, gdyż trwa on kilka pojedynczych mikrosekund.

Kolejnym fundamentalnym procesem w transmisji OFDM jest zastosowanie cyklicznego prefiksu, czyli kopii ostatniej części każdego symbolu, na początku każdego symbolu, co pomaga wyeliminować zakłócenia między symbolami. Jego długość jest tak dobrana, aby była większa niż maksymalne przewidywane opóźnienie kanału przy propagacji wielodrogowej. Jednym ze sposobów destruktywnego wpływu na transmisję jest, podobna do wspomnianej powyżej, technika nadawania z małym wypełnieniem, celowana w obszar ramki zawierający ten element. Alternatywna metoda polega na skonstruowaniu dodatko-

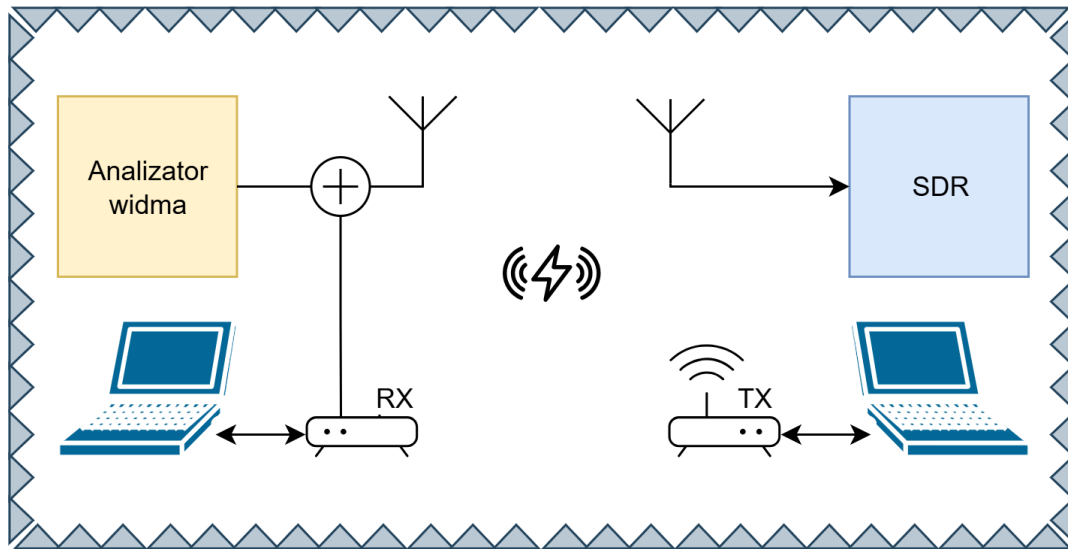
wej ścieżki dla docelowego sygnału OFDM z opóźnieniem dłuższym niż zakładany prefiks. Teoretycznie, urządzenie zakłócające może przechwycić bieżący sygnał OFDM, a następnie wyemitować go z dodatkowym opóźnieniem. W rezultacie agregacja sygnałów docelowego i zakłócającego jest równoważna zanikowi z powodu kanału o nadmiernym rozkładzie opóźnienia [203].

Wspomniane metody wymagają znacznej wiedzy o parametrach sygnału i niejednokrotnie dobrej synchronizacji między nadajnikiem zakłócającym a odbiornikiem. Przy tak dużej różnorodności komercyjnych statków bezzałogowych, które ciągle rozwijają się poza standardowymi protokołami, oraz w obliczu możliwości występowania więcej niż jednego obiektu w strefie ochrony, nie sposób zastosować tych zaawansowanych technik w obecnej pracy. Aby przetestować efektor, tym razem skupiono się na podstawowym podejściu do zakłócania, pozostawiając bardziej świadome metody jako temat dalszych badań.

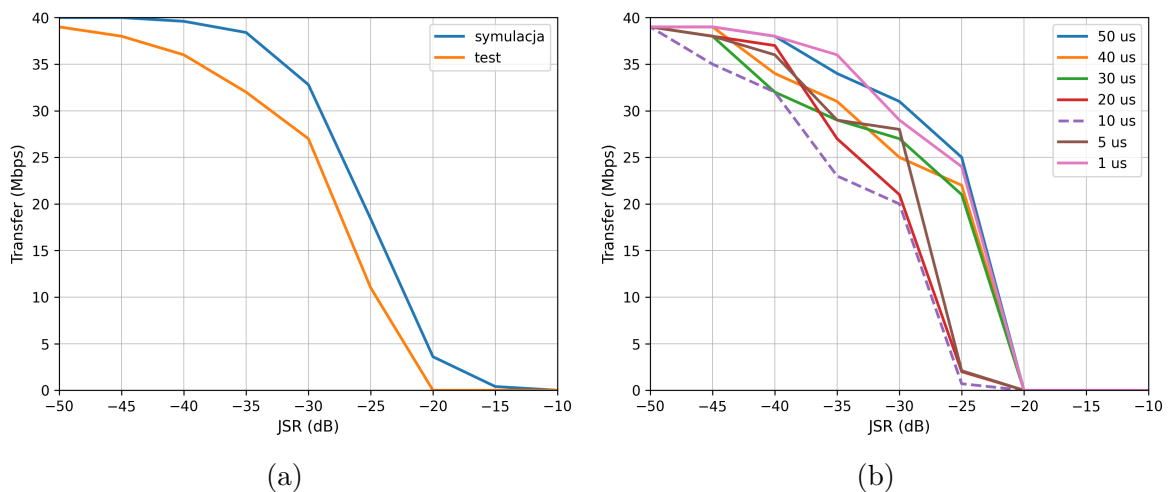
7.2.3 Eksperymenty

W pierwszej sesji eksperymentalnej, w izolowanej komorze semi-bezodbiciowej, zestawiono stanowisko do transmisji bezprzewodowej w trybie protokołu 802.11n, bazujące na dwóch ruterach L23UGSR firmy MikroTik. Badanie to ma odwzorować charakter zakłócania dronów wciąż opartych na protokołach Wi-Fi, dając jednocześnie dostęp do statystyk transferu danych i możliwość wykorzystania zewnętrznych złączy antenowych. Schemat stanowiska przedstawia rysunek 7.10. W sieciach Wi-Fi połączenie ma charakter dwukierunkowy, aby utrzymać aktywność łącza i wysyłać potwierdzenia, ale narzędzia obecne w systemie wewnętrznym modemów pozwalają na mierzenie przepustowości transferu danych niezależnie w obu kierunkach. Z uwagi na to, jedno z urządzeń umownie wyróżniono jako transmitujące (TX), a drugie jako odbierające (RX). Tor antenowy urządzenia odbiorczego będącego celem ataku został rozdzielony analogowo, aby na żywo monitorować zarówno poziom sygnału odbieranego ze ścieżki właściwej, jak i zakłócającej. Ustawienie to posłuży także do oszacowania osiąganego poziomu miary JSR.

Przed rozpoczęciem testów wykonano także symulacje przypadku zakłócania szumowego w środowisku Matlab, korzystając z obiektów wlanHTConfig i wlanTGnChannel. Model komputerowy skonfigurowany był dla parametrów określających 20 MHz szerokość kanału, jedną antenę nadawczą i odbiorczą oraz modulację 64QAM. Rzeczywisty układ nadawczy ustawiony był na pełne pasmo 96 MHz oraz częstotliwość środkową 2445 MHz, a routery pracowały zgodnie z protokołem 802.11n na kanale o szerokości 20 MHz i z częstotliwością środkową 2412 MHz. Poza porównaniem wrażliwości na zakłócenia szumowe, głównym celem przeprowadzonych pomiarów było badanie wpływu czasu powtarzania przebiegu sinusoidalnego w całym paśmie ISM 2,4 GHz na transmisję 802.11n dla techniki przestrajanej. Wyniki eksperymentów zawarte są na rysunku 7.11.

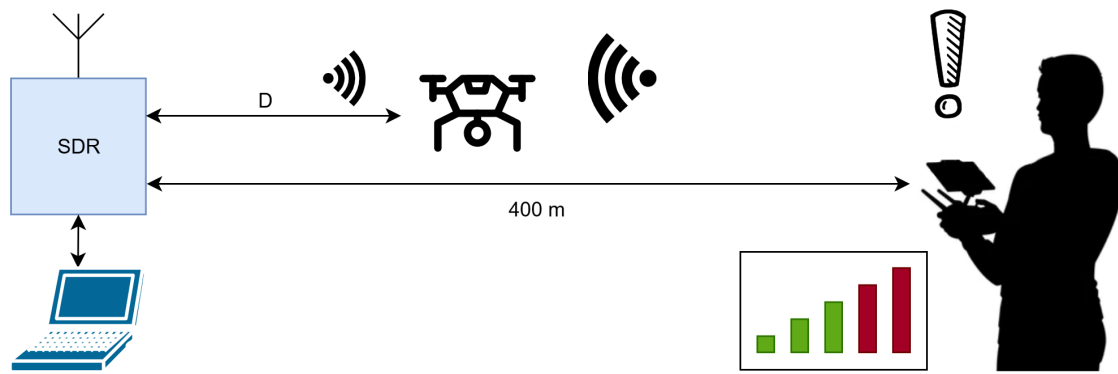


Rysunek 7.10: Stanowisko eksperymentalne badania wpływu zakłócania na przepustowość w protokole 802.11n.



Rysunek 7.11: Zestawienie wyników badania wpływu różnych form zakłócania na szybkość transferu danych dla protokołu 802.11n: (a) wynik symulacji metody szumowej odniesiony do pomiarów, (b) zestawienie różnych czasów przestrajania fali sinusoidalnej.

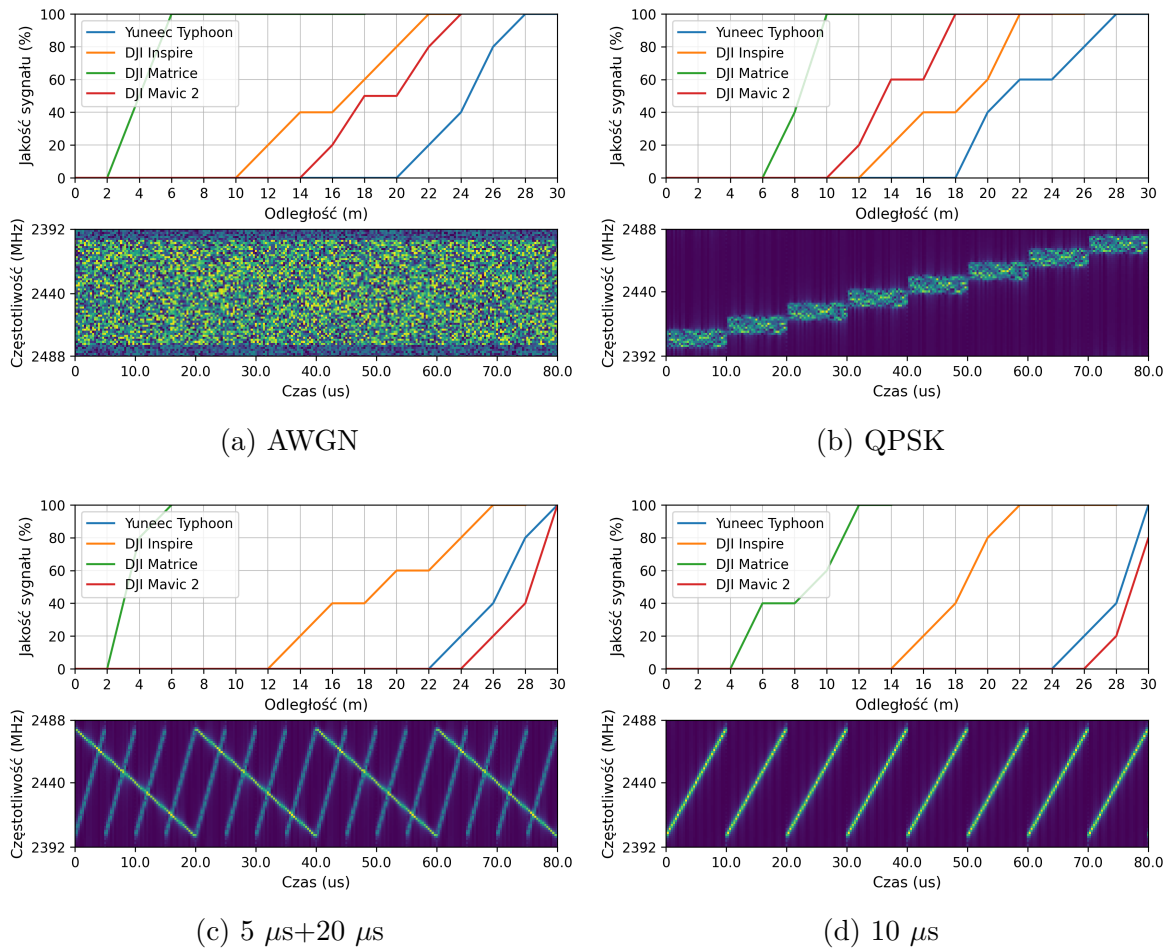
Zarówno symulacja, jak i badania eksperymentalne dla zakłócania szumowego pokazały, że ograniczenia prędkości transferu zaczynają się pojawiać już w okolicy -45 dB wartości JSR. Przepustowość w pomiarze laboratoryjnym spada jednak szybciej, a całkowite odcięcie możliwości przesyłu pojawia się w okolicy -20 dB wartości JSR, podczas gdy dla symulacji następuje to przy sygnale zakłócającym mocniejszym o 5 dB. Wyniki są bardzo zbliżone, a powstałe różnice mogą wynikać z szacunkowego charakteru pomiaru parametru JSR na analizatorze widma oraz z prawdopodobnych dodatkowych odbić od dużej ilości sprzętu rozmieszczonego wewnątrz komory. Dodatkowo podczas nadawania w pełnej szerokości pasma SDR dało się zauważyć fluktuacje poziomu sygnału wyjściowego



Rysunek 7.12: Szkic planu pomiaru wpływu różnych technik zakłócających na bezzałogowe statki powietrzne.

spowodowane nieidealnością końcówki analogowej, przez co wpływ na podnośne w transmisji mógł być nierównomierny, jak w przypadku symulacji. Dla techniki przestrajanej, da się zaobserwować pogłębiające się oddziaływanie zakłóceń przy zmniejszaniu okresu przebiegu fali od $50 \mu\text{s}$ do $20 \mu\text{s}$. Największy jednak wpływ i praktycznie odcięcie możliwości przesyłu danych dla okresu $10 \mu\text{s}$ następuje dla wartości -25 dB JSR , a dalsze zmniejszanie czasu przestrajania tylko pogarsza ten wynik.

W ostatniej sesji pomiarowej odtworzono warunki rzeczywistej ochrony przed wtargnięciami komercyjnych statków bezzałogowych, podobne do przedstawionych w opracowaniu [137]. W zaplanowanym eksperymencie jednak to położenie stacji zakłóceń i operatora było stałe, a wartość mierzona stanowiła odległość między dronem a efektem, wymagana do utraty kontroli nad obiektem. Sytuacja ta przedstawiona jest na rysunku 7.12. W tym eksperymencie nie jest możliwy cyfrowy odczyt jakichkolwiek parametrów związanych z wpływem zakłócania na drona, a jedyną oznaką jest zachowanie obiektu oraz wskazanie poziomu sygnału na aparaturze sterującej operatora, określone w pięciu poziomach. Podczas testów zachowano bezpośrednią widoczność pomiędzy wszystkimi elementami, a dla utrzymania bezpiecznych warunków odległość między nimi nie przekraczała zasięgu linii wzroku. Każdy obiekt poddany został działaniu czterech różnych przebiegów zakłócających, pokrywających pełne pasmo ISM 2,4 GHz, wykorzystano maksymalną moc nadajnika oraz dookólną antenę dipolową. Obok techniki szumowej oraz przestrajanej fali sinusoidalnej z okresem $10 \mu\text{s}$, zastosowano złożenie przeciwstawnych przebiegów o czasie trwania $5 \mu\text{s}$ i $20 \mu\text{s}$, a także sygnał zmodulowany QPSK o szerokości pasma 10 MHz i zmiennym położeniu w widmie co $10 \mu\text{s}$. Okres przestrajanych przebiegów zakłócających dobrany został tak, aby mimo często obecnej w dronach techniki rozpraszania widma z przeskokami częstotliwości, sygnały nadawane nałożyły się na te właściwe co najmniej kilkukrotnie podczas pojedynczej transmisji. Dlatego najdłuższy czas powtarzania przebiegu wynosi $0,08 \text{ ms}$, gdy komendy sterujące w badanych urządzeniach trwają od $0,650 \text{ ms}$ do 2 ms . Opisane przebiegi wraz z wynikami pomiarów zobrazowano na rysunku 7.13.



Rysunek 7.13: Wyniki badań zasięgu zakłócania komercyjnych statków bezzałogowych operujących w pasmie ISM 2,4 GHz.

Dron DJI Matrice jest najcieńszą jednostką z całego zestawienia i przeprowadzone eksperymenty wskazują na jego największą odporność na zakłócenia, niezależnie od dobranej fali radiowej. Największą wrażliwość w jego przypadku udało się zaobserwować na przebieg zmodulowany QPSK, a najmniejszą na AWGN. Obiekt najlżejszy natomiast to DJI Mavic 2, który największą czułość wykazał na przebiegi przestrajane. Wśród przebadanych typów zakłóceń, za najbardziej skuteczny można uznać przebieg z przestrajaną falą sinusoidalną o okresie $10 \mu s$, z uwagi na największą odległość, w której jakość sygnału odbieranego spada do zera dla trzech modeli dronów. Ponieważ pomiar rzeczywistej wartości stosunku sygnału użytecznego i zakłócającego był w takich warunkach utrudniony, oszacowanie zostało wykonane na bazie modelu propagacji wolnej przestrzeni. Przy takim założeniu niezbędne do spowodowania całkowitego rozłączenia komunikacji pomiędzy dronem a operatorem są wartości JSR w granicach od 6 dB do 26 dB w zależności od modelu drona.

Rozdział 8

Podsumowanie

8.1 Wnioski z realizowanych prac

Wprowadzenie bezzałogowych statków powietrznych na rynek komercyjny, dzięki wyjątkowej wszechstronności tych urządzeń i ich stosunkowo niskiej cenie, rozwinęło zupełnie nowe perspektywy w wielu obszarach związanych zarówno z zastosowaniami przemysłowymi, jak i osobistymi. Niska bariera wejścia do społeczności użytkowników systemów bezzałogowych doprowadziła również do pojawienia się nieznanej wcześniej kategorii potencjalnych zagrożeń, nie tylko dla infrastruktury krytycznej, ale również dla życia codziennego.

W pierwszej części prezentowanej rozprawy, na podstawie przeglądu literatury, przedstawiono wady i zalety różnych technik detekcyjnych oraz umotywowano wybór przyjętej ścieżki. Scharakteryzowano podejścia bazujące na sygnałach dźwiękowych, analizie obrazu, układach radarowych oraz rozpoznaniu radiowym. Wyciągnięte wnioski wykazują, że skuteczność metod akustycznych jest ograniczona przez hałas miejski, wiatr i warunki atmosferyczne, a podejście to nie ma zastosowania w przypadku dronów szybujących. Rozpoznanie obrazowe wymaga kamer o wysokiej rozdzielczości i zaawansowanej optyki, a w celu monitorowania otoczenia niezbędny jest ciągły ruch głowic obserwacyjnych. Mimo iż techniki uczenia maszynowego dobrze radzą sobie z rozpoznawaniem standardowych obiektów dronowych, to wciąż pojawiają się nowe konstrukcje oraz formy stworzone po to, aby je oszukać. Technika radarowa, będąca najbardziej kosztownym rozwiązaniem, pozwala wykrywać i śledzić wiele obiektów jednocześnie, ale jej dokładność może być ograniczona przez mniejsze rozmiary dronów, operowanie na niskich wysokościach czy niską prędkość lotu i środowisko miejskie. Na ograniczenie skuteczności i zasięgu działania wybranej metody radioelektronicznej spory wpływ ma wysokie zagęszczenie nadajników oraz skomplikowane środowisko propagacyjne. Podejście to jest wprawdzie nieskuteczne w przypadku operacji bez kontroli operatora w czasie rzeczywistym, jednakże scenariusz ten nie występuje często, gdyż podstawą wielu nieuprawnionych przypadków użycia dro-

nów jest możliwość transmisji obrazu na żywo i korekcji toru lotu maszyny. Jako że żadna z analizowanych metod stosowanych samodzielnie nie daje pewności wykrycia niepożądanych statków bezzałogowych, rozwój każdej z indywidualnych technik jest wciąż niezwykle istotny, a osiągnięcie pełnej świadomości sytuacyjnej wymaga konstrukcji układów wielosensorowych. Szczegółowa synteza prac badawczych pozwoliła na zgrupowanie opisanych metod detekcyjnych pod kątem analizy sygnałów w formie protokołu, w dziedzinie czasu, w dziedzinie częstotliwości oraz w zapisie za pomocą spektrogramu. Najbardziej skuteczną i uniwersalną metodą, szczególnie przy niskim współczynniku sygnał-szum oraz w obecności innych transmisji, okazała się ta ostatnia, dlatego dalsze prace ukierunkowano w stronę rozwoju algorytmów uwzględniających to podejście.

Skuteczny proces detekcji stanowi dopiero pierwszy krok w obronie przed wtargnięciami bezzałogowych statków powietrznych w chroniony obszar. Podejście radioelektroniczne to jedyny zestaw technik, który może posłużyć zarówno w fazie detekcji, jak i neutralizacji, nawet przy braku bezpośredniej widoczności optycznej celu oraz działając równocześnie na wielu intruzów. Podejmując się przeglądu literatury dotyczącej przeciwdziałania statkom bezzałogowym, podział na poszczególne techniki, takie jak zakłócanie szumem białym, falą ciągłą, przestrajane, czy świadome, był utrudniony z uwagi na mniejszy zasób przedmiotowych opracowań oraz różne warunki odniesienia dla przeprowadzanych eksperymentów. Podstawą zgrupowania w tej kategorii, tak jak w dalszej części rozprawy, było przyjęcie podziału na konkretne typy transmisji, które stają się celem ataków zakłócających. Wnioski płynące z prac traktujących bezpośrednio o testach komercyjnych statków bezzałogowych w środowisku rzeczywistym wskazały na odmienne zachowania dronów w momencie pojawienia się zakłóceń sygnałów nawigacji satelitarnej. Niektóre modele przechodziły z trybu lotu w tryb zawisu, inne natychmiast rozpoczynały procedurę lądowania, czy nawet nie podejmowały próby startu, gdy zakłócenie odbywało się odpowiednio wcześniej. W tej kategorii najczęściej pojawiały się próby zakłócania świadomego oraz przestrajanego, co uwzględnione zostało w późniejszych eksperymentach własnych. Warte podkreślenia były także badania w środowisku rzeczywistym, wskazujące na wpływ charakterystyki samej anteny odbiornika nawigacyjnego, a co za tym idzie, wysokości lotu platformy, na zasięg nadajników zakłócających.

W sekcji opisującej proces rozwoju fizycznego prototypu, opisano koncepcję radia definiowanego programowo, przedstawiono najpopularniejsze modele dostępne na rynku, a wybrany układ został zarysowany bardziej szczegółowo. W zestawieniu z elementami z podobnej kategorii cenowej, prototyp osiągnął pasmo natychmiastowe pozwalające na obserwację pełnego zakresu pasma ISM 2,4 GHz, bez potrzeby przestrajania lub multiplikacji urządzeń. Układ konkurencyjny posiada wprawdzie przewagę w kontekście możliwości detekcji bardzo słabych sygnałów, jednak zakres pracy liniowej wybranej końcówki analogowej, jak pokazały symulacje, wystarcza w zupełności do zapewnienia odpowiedniego pokrycia przestrzeni w koncepcji systemu rozproszonej detekcji. Wprowadzony do czę-

ści sprzętowej tor wstępnego przetwarzania sygnału, obejmujący generację transformaty czasowo-częstotliwościowej, pozwolił na przeznaczenie całych zasobów komputera towarzyszącego na obliczenia związane z dalszymi etapami klasyfikacji transmisji. Największą zidentyfikowaną wadą tego elementu sprzętowego było ograniczenie górnego zakresu pracy do 3,8 GHz. Dobranie zewnętrznego przemiennika częstotliwości, wraz z kolejnymi modyfikacjami oprogramowania polegającymi na przyspieszeniu przestrajania częstotliwości środkowej, niewielkim kosztem zniwelowało ten mankament, wprowadzając dodatkowo potencjalną możliwość obserwacji dwóch pasm równoległe. W standardowych urządzeniach z tej kategorii, jednoczesna praca dwóch kanałów odbiornika na różnych częstotliwościach środkowych nie jest możliwa z uwagi na wewnętrznie współdzielony układ PLL. Na wczesnym etapie projektu, stosowność wprowadzonych modyfikacji przetestowana została pod kątem manualnej obserwacji sygnałów jeszcze bez wprowadzania zaawansowanych algorytmów detekcyjnych. Prezentowane urządzenie wykazało skuteczność w przypadku estymacji podstawowych parametrów transmisji związanych z charakterystycznym dla dronów trybem pracy z przeskokami częstotliwości oraz przy monitorowaniu zajętości kanałów sieci komórkowej podczas strumieniowania obrazu wysokiej jakości.

Badania symulacyjne, przeprowadzone w odniesieniu do obiektu przemysłowego o dużej powierzchni, miały na celu pokazanie słuszności koncepcji rozproszonego podejścia do ochrony przed wtargnięciami systemów bezzałogowych. W procesie tym uwzględniona została trójwymiarowa struktura budynków, a estymacja zjawisk propagacyjnych, takich jak tłumienie, odbicia i refrakcja, odbywała się za pomocą techniki analizy promieni. W kontekście detekcji istotnym było zaprezentowanie wpływu zabudowań i oszacowanie poziomu sygnału dla rozmieszczonych na obiekcie odbiorników, także aby potwierdzić zgodność z wejściowym zakresem pracy końcówki analogowej przygotowanego prototypu. Przy założonych scenariuszach wtargnięcia systemu bezzałogowego, eksperymenty wykazały większą stabilność poziomu sygnału dla zestawienia pięciu detektorów rozmieszczonych w granicach obiektu niż dla detektora centralnego. W przypadku redukcji kosztów pojedynczego węzła jednak element centralny nie powinien być wykluczany, gdyż zapewni redundancję i dobre uzupełnienie całości systemu. W aspekcie zakłócania sygnałów nawigacji satelitarnej istotnym aspektem symulacji było uwzględnienie charakterystyki promieniowania anteny odbiorczej, która bardzo mocno wpłynęła na możliwy do uzyskania stosunek sygnału zakłócającego do właściwego. Było to szczególnie widoczne przy większych wysokościach, kiedy promień generowany z poziomu ziemi trafiał w minimum wzmocnienia anteny. Dlatego, podobnie jak w przypadku próby oddziaływania na tor odbiorczy sygnałów sterujących, zaproponowano rozmieszczenie elementów zakłócających w bezpośredniej bliskości chronionego obszaru lub zwiększenie mocy nadawania poprzez zewnętrzne układy analogowe.

Przegląd publicznie dostępnych baz danych sygnałów dronowych wykazał, że większość z nich nie jest odpowiednia do ewaluacji przyjętej strategii identyfikacji opierającej się na detekcji charakterystycznej preambuły ramki radiowej. Część z nich zawiera fragmen-

taryczne dane, które wprowadzie dają ogólny obraz widma, jednakże często zdarzają się niespodziewane ubytki próbek wynikające ze strat interfejsu połączeniowego pomiędzy radiem a komputerem. Jest to znana przypadłość, której opanowanie również było celem prac nad modyfikacją oryginalnego oprogramowania układu SDR. Inne zestawy danych, których nie sposób wykorzystać, oparte były na odmiennym urządzeniu próbkującym lub w sposób znaczny utrudniały oznaczenie transmisji pochodzących z różnych źródeł. Wybrana baza jednak opierała się na nagraniach pozyskanych w komorze bezodbiciowej, co po uzupełnieniu syntetycznymi danymi dało zbiór treningowy, który łatwo oznaczyć oraz przeprowadzić podział z uwzględnieniem SNR. Ciągły rozwój bazy danych został uwzględniony jako istotny kierunek dalszych prac.

Zaproponowane podejście do detekcji, oparte na klasyfikacji regionu preambuły, odmiennie jest od wielu opracowań bazujących także na zapisie czasowo-częstotliwościowym. Podejścia innych autorów często traktowały wycinek widma, w postaci dwuwymiarowego obrazu, jako całość, a klasyfikacji dokonywano na podstawie wiedzy, czy w danym momencie występowała transmisja systemu bezzałogowego, czy nie. Technika ta wydawała się skuteczna jeszcze kilka lat temu, kiedy rozróżnienia pomiędzy modelami dronów dokonywano przy braku innych sygnałów, lub klasyfikacja opierała się na tym, że niektóre modele nadają sygnał w określonych kanałach. W najnowszych artykułach problem ten został zauważony i coraz częściej podejmuje się temat detekcji w obecności zakłóceń lub przy niskiej wartości stosunku sygnał-szum. W proponowanym podejściu starano się uniezależnić od obecności innych sygnałów w paśmie przetwarzania, w celu uproszczenia samego detektora i optymalizacji czasu przetwarzania. Pierwszym krokiem było wybranie metody opartej na spektrogramie, która w odróżnieniu od analizy w dziedzinie czasu dawała wstępne rozdzielanie transmisji pracujących na różnych częstotliwościach środkowych. Kolejnym była natomiast selekcja jedynie wycinka widma poddanego klasyfikacji, aby ograniczyć wymagane zasoby układu obliczeniowego.

Algorytm decyzji binarnej przy podejściu dwuetapowym wykazał zdecydowanie krótszy czas przetwarzania niż w przypadku metody jednostrzałowej, jednak wymagał podziału zadań pomiędzy różnymi fazami, co utrudniało kompleksową ocenę tego procesu. W etapie pierwszym zastosowano detektor bazujący na progowaniu energii o uniwersalnym charakterze, który nie wymaga wcześniejszej wiedzy o poszukiwanym sygnale, w celu podjęcia pierwszej decyzji o rozróżnieniu sygnału użytecznego od szumu tła. Zastosowano tu podejście adaptacyjne, gdzie nie jest konieczne parametryzowanie algorytmu ani wyznaczanie predefiniowanego progu. Wybrano także sposób, w którym jedna wartość progu obliczana jest dla całego zakresu częstotliwości, co w stosunku do progowania lokalnego minimalizuje szanse pominięcia wąskopasmowych transmisji, ale może spowodować zagubienie sygnałów o niewielkiej mocy w przypadku braku płaskości widma. Dla etapu drugiego przebadano kilka metod z kategorii algorytmów uczenia maszynowego, w których klasyfikacji poddano, przygotowane w fazie poprzedniej, regiony zainteresowania o zróżnicowanym rozmiarze.

Najskuteczniejsza okazała się prosta, dwuwarstwowa sieć neuronowa, a przetwarzanie nawet dla obszaru większego było szybsze niż czas trwania najkrótszej ramki radiowej w zbiorze. Większy stopień złożoności sieci nie spowodował już polepszenia dokładności klasyfikacji binarnej. Skuteczność tej metody ograniczona jest zdecydowanie przez stopień detekcyjny, który dla niskich wartości stosunku sygnał-szum nie był w stanie dostarczyć danych dla etapu klasyfikacji binarnej. Aby potwierdzić skuteczność przyjętej koncepcji w środowisku zbliżonym do rzeczywistego, wybrany model został przystosowany do implementacji w komputerze wbudowanym. Niezbędny do tego proces kwantyzacji, w którym nastąpiła zmiana operacji zmiennoprzecinkowych na stałoprzecinkowe wraz ze zmniejszeniem zakresu bitowego, obniżył minimalnie jakość klasyfikacji, co nie wpłynęło jednak znacząco na finalną dokładność rozwiązania.

Optymalizacja algorytmu detekcji dronów pod kątem minimalizacji złożoności obliczeniowej, może w praktyce niedługo okazać się zbędna, z uwagi na ciągły wzrost mocy obliczeniowej komputerów wbudowanych i pojawianie się sprzętowych akceleratorów AI. Idąc za tym trendem, w dodatkowej serii eksperymentów porównano ze sobą modele YOLO kolejnych generacji o różnym stopniu gęstości sieci. Ograniczono się tu do dwóch pierwszych poziomów, gdyż proces trenowania dla tego drugiego przekraczał już 130 godzin. W tej metodzie także zastosowano podejście bazujące na oznaczeniu samej preambuły, tym razem jednak klasyfikacji poddawany nie był wycinek widma, a pełny spektrogram odpowiadający wielkością warstwie wejściowej sieci. Niewątpliwym atutem tej techniki jest jednoczesna detekcja i klasyfikacja, dzięki czemu można jednoznacznie ocenić algorytm pod względem parametrów jakościowych. Zapis sygnałów radiowych, próbkowanych z wysoką częstotliwością, generuje znacznie większą ilość danych niż obraz z kamery, toteż nawet dla najprostszej sieci w tej kategorii nie zbliżono się do czasu obliczeń, który w tym zastosowaniu, uważany mógłby być za przetwarzanie w czasie rzeczywistym. Ciekawą obserwację stanowią natomiast wyniki jakościowe, które pokazują brak wyraźnej przewagi dla serii sieci o wyższym stopniu gęstości. Dodatkowo, z finalnego zestawienia parametrów można wyciągnąć wniosek, iż najnowsze architektury sieci, optymalizowane do standardowej bazy obrazów, wcale nie sprawdzają się lepiej w przypadku tego specyficznego zadania, jakim jest klasyfikacja spektrogramów.

W ostatniej części rozprawy skoncentrowano się na przeciwdziałaniu komercyjnym statkom bezzałogowym przy pomocy emisji fal radiowych, poprzez opracowany efektor. Na potrzeby badań w aspekcie sygnałów nawigacji satelitarnej zestawiono stanowisko, bazując na sygnałach rzeczywistych sumowanych analogowo z falami zakłócającymi. Podczas eksperymentów zwiększano moc nadajnika, sterując wzmocnieniem układu radiowego, oraz obserwowano współczynniki odnoszące się do wewnętrznych pomiarów parametru C/N_0 , liczby satelitów i poprawności wyliczenia pozycji. Korzystając wyłącznie z konstelacji GPS, odbiornik wykazywał już znaczną reakcję na sygnały zakłócające przy 60% wystawienia dla techniki świadomej oraz przestrajanej. Odnosząc te wyniki do symulacji,

efektory nadające z dostępną mocą, rozmieszczone w tych samych miejscach co detektory, nie zapewniają wystarczającej ochrony przy podejściach na dużych wysokościach. Rozmieszczenie efektorów w bezpośredniej bliskości krytycznych instalacji podatnych na atak może jednak dać pożądane efekty niezależnie od wysokości. Odbiorniki nawigacji satelitarnej stosowane w najnowszych modelach dronów potrafią już jednak wykorzystywać więcej konstelacji w sposób równoległy, a wtedy ich zakłócenie przy dostępnej mocy staje się trudniejsze. Pokazano to w kolejnym eksperymencie, badając dodatkowo wpływ różnych okresów przestrajania na poszczególne konstelacje. Dla tego typu fali wytrącenie odbiornika ze zdolności wskazywania pozycji wystąpiło jedynie dla pełnej mocy wystrojenia efektora. W ostatnim eksperymencie w tej kategorii najskuteczniejsza kombinacja fal sinusoidalnych zaczęła oddziaływać na odbiornik przy 80% wystrojenia, co przekłada się na około 58 dB stosunku JSR. Umieszczenie efektora w bezpośredniej bliskości chronionego miejsca powoduje, że zakłócanie staje się skuteczne, kiedy dron znajduje się nad celem, ale poniżej 64 m, a przy podejściu na wysokości 8 m odległość wzrasta do ponad 100 m. Poza stosunkowo niewielką mocą nadawania samego efektoru, ma na to wpływ głównie kierunkowa charakterystyka anteny GNSS, która skutecznie tłumi sygnały nadawane z ziemi.

Aby potwierdzić wpływ efektoru na sygnały komunikacyjne, w pierwszej kolejności zestawiono stanowisko bazujące na dwóch ruterach sieciowych pracujących w trybie protokołu 802.11n. Miało to odwzorować charakter zakłócania dronów wciąż opartych na transmisjach Wi-Fi, dając jednocześnie dostęp do statystyk transferu danych. Wyniki pomiarów dla techniki zakłócania szumowego są zgodne z symulacjami i wskazują, że niezbędny do poważnego ograniczenia szybkości transferu jest poziom JSR wynoszący -20 dB. Analiza wpływu zakłócania przestrajanego natomiast wykazała, że stosując okres równy 10 μ s, do uzyskania podobnego wyniku wystarczająca jest wartość -25 dB JSR. Odnosząc te wartości do symulacji ochrony obiektu, to niezależnie od wysokości drona można liczyć na skuteczne oddziaływanie układu zakłócającego już w okolicy punktu trzeciego na ścieżce podejścia. W ostatniej sesji pomiarowej nastąpiło przeniesienie eksperymentów do warunków zbliżonych do rzeczywistych, w których wykorzystano cztery modele komercyjnych statków bezzałogowych, aby zbadać odległość, na jaką mogą one zbliżyć się do efektoru przy różnym typie emisji. Wśród testowanych dronów jeden okazał się zdecydowanie bardziej odporny na zakłócenia od reszty. Oszacowany poziom JSR niezbędny dla skutecznego przeciwdziałania wynosił dla niego nawet 26 dB, natomiast dla drona najbardziej czułego wystarczający był już poziom 6 dB. Wysoki stopień odporności jednego z testowanych urządzeń wskazuje na konieczność stosowania mocniejszych sygnałów zakłócających lub anten kierunkowych o dużym wzmacnieniu.

8.2 Ocena stopnia realizacji przyjętych celów

Głównym celem przedstawionej rozprawy było zaproponowanie systemu wykrywania oraz przeciwdziałania nieuprawnionemu wykorzystywaniu komercyjnych bezzałogowych statków powietrznych przy pomocy środków walki elektronicznej. Dążenie do realizacji przyjętych założeń opierało się na pięciu tezach badawczych, z których każda została indywidualnie udowodniona.

Możliwa jest realizacja układu detekcji oraz zakłócania operacji bezzałogowych statków powietrznych na podstawie informacji z modułu radia definiowanego programowo.

Przegląd literatury przeprowadzony w pierwszej części rozprawy wykazał, iż podejście uwzględniające wykrywanie emisji fal elektromagnetycznych pochodzących od statków bezzałogowych jest metodą zarówno często analizowaną w środowisku naukowym, jak i chętnie wykorzystywaną jako element komercyjnych systemów antydronowych. Spowodowane jest to faktem, iż ogromna liczba incydentów z udziałem dronów wynika z nieświadomego użytkowania urządzeń komercyjnych lub opiera się na pewnej potrzebie obserwacji terenu, co nieodłącznie związane jest z transmisją bezprzewodową obrazu na żywo oraz wymogiem precyzyjnego sterowania obiektem. Dodatkowo, jest to jedyna technika, w której to samo urządzenie bazowe spełniać może rolę detektora i efektora, a poszukiwany obiekt wykryty może zostać w trakcie zestawiania połączenia bezprzewodowego jeszcze przed oderwaniem się od ziemi. Choć ta metoda może być nieskuteczna dla specjalnie dostosowanych urządzeń, które nie wymagają fal radiowych do komunikacji i sterowania ani nie wykorzystują systemów nawigacji satelitarnej, to wciąż żadna z innych analizowanych technik samodzielnie nie jest w stanie zapewnić pełnej ochrony.

Możliwa jest realizacja systemu detekcji oraz zakłócania komercyjnych dronów, bazującego na gotowych układach elektronicznych i modyfikacji oryginalnego oprogramowania.

Zrealizowane prace w pełni pokrywają przyjęte założenia dotyczące części sprzętowej, gdyż doprowadzono do powstania funkcjonalnego prototypu urządzenia bazującego na gotowych elementach elektronicznych. Kluczowym podzespołem jest tu układ radia programowalnego, który posiada zarówno tor nadawczy, jak i odbiorczy, odpowiedni do działania z szerokim pasmem natychmiastowym. Zaletą wyboru tego urządzenia, w przeciwieństwie do stosowanych alternatywnie przyrządów laboratoryjnych, jest możliwość dostosowania sterowania końcówką analogową z poziomu wewnętrznego oprogramowania bez dużego udziału komputera zewnętrznego, co zostało zaprezentowane na przykładzie przyspieszenia obsługi przestrajania częstotliwości środkowej.

Zastosowanie architektury sprzętowo-programowej i zwiększenie udziału macierzy programowalnych bramek logicznych w przetwarzaniu sygnałów, w porównaniu do klasycznej koncepcji radia programowalnego, pozwoli na optymalizację procesu detekcji oraz zakłócania.

Klasyczna koncepcja radia programowalnego zakłada dostarczenie przez sprzętowy moduł odbiorczy próbek sygnału w surowej postaci do komputera zewnętrznego, tak aby cała analiza i przetwarzanie mogły odbywać się w sposób zapewniający tylko łatwe modyfikowanie na warstwie oprogramowania wysokiego poziomu. W kontekście modułu nadawczego sytuacja wygląda podobnie, a próbki dla obu torów przechodzą przez półduplexowy interfejs szeregowy. Przeniesienie części operacji, oryginalnie wykonywanych przez kontroler zewnętrzny, do warstwy macierzy bramek logicznych pozwoliło na zmniejszenie obciążenia i wpływu latencji interfejsu przesyłu danych, co skutkuje nie tylko możliwością wykorzystania pełnego natychmiastowego pasma obserwacji, ale także automatyzacji procesu przestrajania i kalibracji. Dodatkowo, implementacja segmentu transformacji czasowo-częstotliwościowej w macierzy programowalnych bramek logicznych pozwoliła na przeznaczenie pełnych zasobów komputera wbudowanego na dalsze obliczenia związane z procesem detekcyjnym. Przyjęty w torze nadawczym format odtwarzania przebiegu z wewnętrznej pamięci układu radiowego nie wprowadził również redukcji przepustowości półduplexowego interfejsu komunikacyjnego podczas generacji fali zakłócającej, jednocześnie zapewniając elastyczność w jej doborze. Pozostawiając w ten sposób przestrzeń na transfer próbek sygnału w kierunku przeciwnym, możliwe jest potencjalnie zakłócanie sygnałów nawigacji satelitarnej przy jednoczesnym nasłuchu częstotliwości komunikacyjnych przeznaczonych dla komercyjnych statków bezzałogowych, przy pomocy jednego urządzenia.

Optymalizacja procesu detekcji, pod względem minimalizacji czasu przetwarzania, może zostać zrealizowana dzięki analizie tylko fragmentów ramek radiowych.

Zaprezentowane w tym opracowaniu metody opierają się na analizie spektrogramu, który jest często wybieraną formą reprezentacji widma w procesie klasyfikacji sygnałów radiowych. Przedstawione podejście nie opiera się jednak na próbie całościowego przetwarzania pełnego okna czasowego zawierającego wiele transmisji, a skupia się na interpretacji początkowego fragmentu wykrytej ramki radiowej. Obszar ten, zwany preambułą, dzięki swojej charakterystycznej formie służy zazwyczaj do odróżnienia sygnału właściwego od szumu w odbiorniku w procesie korelacji. Dla zaproponowanej metody dwuetapowej czas przetwarzania sieci neuronowej został skutecznie zminimalizowany, dzięki redukcji rozmiaru macierzy w warstwie wejściowej poprzez wstępną selekcję wybranego obszaru zainteresowania. Przeprowadzone eksperymenty wykazały wysoką skuteczność tej formy klasyfikacji binarnej, a ograniczeniem w tym procesie dla niskiej wartości stosunku sygnał-szum okazał się etap detekcji energii.

System rozproszonej detekcji będzie miał przewagę w terenie zabudowanym nad systemem z detektorem centralnym oraz pozwoli na stworzenie skalowalnej sieci automatycznego nadzoru.

Zaproponowane rozwiązanie sprzętowo-programowe oferuje minimalizację kosztów pojedynczego urządzenia oraz lokalne przetwarzanie danych ograniczające wymagania przepustowości sieci połączeniowej prowadzącej do centrum decyzyjnego. Wpisuje się w to nowoczesne trendy budowania modułowych systemów o skalowalnym charakterze, ze zminimalizowanym współczynnikiem ryzyka spowodowanego dezaktywacją pojedynczego węzła. Przeprowadzone symulacje, uwzględniające możliwe osiągi systemów bezzałogowych, wskazują, iż dla wielkopowierzchniowych obiektów przemysłowych jest to rozwiązanie bardziej korzystne z uwagi na skomplikowane środowisko propagacyjne dla systemu scentralizowanego.

8.3 Kierunki dalszych badań

Zagadnienie poruszone w przedstawionym opracowaniu jest tematem szerokim, a szybki postęp technologiczny w tej dziedzinie stwarza wiele okazji do ciągłego doskonalenia przedstawionych technik. Sprawia to, że kierunki dalszych badań można zarysować zarówno dla całego systemu, jak i dla indywidualnych jego komponentów.

Dla elementu sprzętowego rozwój opierać może się na dalszym zwiększeniu udziału układu programowalnej macierzy bramek w procesie analizy sygnału oraz zastosowaniu końcówki analogowej nowej generacji, oferującej próbkowanie bezpośrednie. Jest to naturalny krok w podążaniu za innowacjami technicznymi, pozwalającymi na zwiększanie pasma natychmiastowego i zmniejszanie latencji przetwarzania. Alternatywnie, nie zmieniając końcówki analogowej, prace programistyczne ukierunkowane mogą być na implementację sieci neuronowych na dedykowanych jednostkach komputerów wbudowanych.

Myśląc o dalszym rozwoju części detekcyjnej, duży potencjał widać w budowaniu bazy sygnatur radiowych, która powinna być ciągle aktualizowana zarówno o dane pochodzące z rzeczywistych systemów, jak i te generowane syntetycznie. W oparciu o nią można tworzyć nowe modele decyzyjne, trenowane i testowane dla scenariuszy o większym zagęszczeniu środowiska elektromagnetycznego, aby maksymalizować dokładność detekcji przy odpowiednim stopniu optymalizacji czasu przetwarzania. Dodatkowo, jako że w eksperymentach uwzględniono jedynie detekcję binarną, kolejnym oczywistym krokiem jest zbadanie możliwości klasyfikacji konkretnych modeli dronów poprzez centrum fuzji danych o większej mocy obliczeniowej, co pozwoli dobrać metody zakłócania zoptymalizowane dla konkretnego typu urządzenia.

Biorąc pod uwagę aspekt efektora, niewiele przestrzeni poświęcono na dobór optymalnych fal zakłócających dla poszczególnych zadań, gdyż stanowi to wydzielone zagadnienie

wymagające także teoretycznej analizy modulacji stosowanych w systemach bezzałogowych. W temacie samej strategii przeciwdziałania natomiast, niewątpliwym krokiem naprzód będzie zmiana w kierunku zakłócania świadomego, które pozwoli nie tylko zaoszczędzić znaczną część energii, ale także nie wpłynie negatywnie na systemy radiowe znajdujące się w okolicy wtargnięcia.

Podchodząc do tematu jak do systemu, należy pomyśleć o metodzie automatycznej optymalizacji rozmieszczenia poszczególnych jego elementów w rzeczywistym zastosowaniu. Podejście to powinno uwzględniać nie tylko uwarunkowania propagacyjne czy urbanistyczne, ale także aspekty związane z charakterystyką użycia systemów bezzałogowych w sposób nieuprawniony. Pamiętać należy także, że ochronę na wysokim poziomie mogą zapewnić tylko systemy heterogeniczne, więc opracowanie standardów wymiany informacji zapewni łatwiejszą fuzję danych między komponentami różnego typu.

Spis rysunków

3.1	Poziom sygnału w zależności od odległości przy założeniu modelu tłumienia wolnej przestrzeni. Dla częstotliwości 2,4 GHz przyjęto moc początkową 20 dBm, a dla częstotliwości 5,8 GHz moc początkowa to 14 dBm.	27
3.2	Graficzna prezentacja macierzy pomyłek dla problemu klasyfikacji binarnej.	37
4.1	Podział na klasy dla komercyjnych dronów do 25 kilogramów w kategorii otwartej [94].	44
4.2	Globalna alokacja pasm radiowych nie wymagających licencji [99].	46
4.3	Zapis czasowo-częstotliwościowy izolowanego sygnału dronowego. Kanał transmisji szerokopasmowej posiada stałą częstotliwość środkową, podczas gdy kanał sterowania wykonuje okresowe przeskoki.	47
4.4	Reprezentacja budowy ramki protokołu 802.11g, z zaznaczonymi podziałami na elementy składowe.	49
4.5	Podział pasm częstotliwości pomiędzy poszczególne systemy nawigacji satelitarnej [103].	51
5.1	Architektura modelowego układu SDR firmy Lime Microsystems.	66
5.2	Budowa wewnętrzna AFE LMS7002M [153].	66
5.3	Budowa wewnętrzna układu FPGA [154].	68
5.4	Budowa wewnętrzna kontrolera SuperSpeed USB FX3 [155].	69
5.5	Układy z rodziny LimeSDR [153].	69
5.6	Układy USRP z serii B [157].	70
5.7	Urządzenie USRP X310 [157].	71
5.8	Schemat blokowy zmian architektury FPGA wewnątrz układu SDR, na przykładzie toru odbiorczego.	74
5.9	Schemat blokowy elementu wyliczającego aproksymację modułu liczby zespolonej na podstawie zależności 5.2.	76
5.10	Schemat blokowy elementu przekształcającego moduł liczby zespolonej na zapis w skali logarytmicznej zgodnie z zależnością 5.4.	78
5.11	Przykładowe spektrogramy pozyskane z sygnałów dostarczonych przez badane urządzenia.	79

5.12	Zapis pojedynczej ramki transmisji danych drona w dziedzinie częstotliwości, przy użyciu dokładnych i przybliżonych technik oraz całkowity błąd przybliżenia.	80
5.13	Porównanie prototypu z urządzeniem referencyjnym w kontekście niezbędnej mocy sygnału wejściowego dla osiągnięcia danego SNR: (a) stanowisko pomiarowe, (b) zestawienie wyników.	81
5.14	Pomiary laboratoryjne toru nadawczego LimeSDR-USB: (a) moc sygnału wyjściowego dla pojedynczego tonu w pełnym zakresie przestrajania, (b) zależność mocy wyjściowej od poziomu wysterowania dla pożądanых częstotliwości zakłócania.	82
5.15	Znormalizowany błąd średniokwadratowy pomiaru przerwy w transmisji FHSS zrealizowany w warunkach zbliżonych do rzeczywistych.	83
5.16	Schemat blokowy prototypu SDR ze zwiększonym udziałem FPGA w procesie detekcji i przeciwdziałania komercyjnym bezzałogowym statkom powietrznym.	84
5.17	Zapis procesu rekonfiguracji PLL w tej samej skali dla oryginalnego oprogramowania i pojedynczej wartości rejestru oraz zmodyfikowanego oprogramowania i pełnego zestawu rejestrów.	86
5.18	Wartości próbek po zmianie częstotliwości środkowej odbiornika obrazujące proces korekcji składowej stałej w oryginalnym i zmodyfikowanym oprogramowaniu.	87
5.19	Zasada działania procesu przemiatania częstotliwości sterowanego z wewnętrznej struktury FPGA.	89
5.20	Zewnętrzna przystawka umożliwiająca rozszerzenie zakresu częstotliwości LimeSDR-USB oraz równoległą pracę w dwóch kanałach oparta na RFFC5071A [168].	91
5.21	Wyniki pomiarów określające poziom sygnału referencyjnego w dBm odniesiony do dBFS dla różnych częstotliwości środkowych i danej szerokości pasma.	92
5.22	Różnica między mocą wejściową generatora sygnału a odczytem z przygotowanego sensora po kalibracji.	93
5.23	Estymacja ruchu sieciowego 'downlink' w pasmach 4G/LTE w dzień i w nocy w terenie mocno zurbanizowanym.	96
5.24	Estymacja ruchu sieciowego 'uplink' w paśmie B7 z podziałem na konkretnych operatorów komórkowych. Aktywacja strumieniowania wideo pokazuje zmianę charakteru obciążenia sieci podczas przesyłu dużej ilości danych. .	96

6.1	Mapa zakładu Bumar Łabędy z oznaczeniem stacji energoelektrycznych i trasy możliwego wtargnięcia z trzech stron. Punkty niebieskie $A - G$ oznaczają rozmieszczenie sensorów, punkty czerwone natomiast to ścieżka podejścia z wyznaczonymi miejscami wykonania estymacji poziomu sygnału.	99
6.2	Wyniki symulacji metodą śledzenia promieni określające poziom sygnału w odbiornikach: (a,b) dla ścieżki I , (c,d) dla ścieżki II , (e,f) dla ścieżki III .	100
6.3	Koncepcja skalowalnej detekcji rozproszonej dla obiektu wielkopowierzchniowego [18].	101
6.4	Łańcuch detekcji w podejściu rozproszonym z podziałem na miejsce wykonywania obliczeń: (a) akwizycja sygnału analogowego i generowanie spektrogramu, (b) detekcja obecności drona i wybór istotnych fragmentów widma, (c) dalsza analiza w centrum fuzji danych.	102
6.5	Proces ekstrakcji ramek sygnałów radiowych ze spektrogramu.	106
6.6	Prezentacja obliczeń wartości progowej dla algorytmu Otsu i NPAQM wraz z krzywymi detekcyjnymi.	110
6.7	Różne algorytmy filtrowania zastosowane do segmentu spektrogramu i odpowiadające im wyniki procesu doboru prostokąta ograniczającego. . . .	111
6.8	Przykładowe wartości parametru IoU dla pola ograniczającego wykrytą transmisję radiową, wyświetlane na wyciętych obszarach spektrogramu. . .	112
6.9	Prawdopodobieństwo detekcji w funkcji SNR dla różnych parametrów maski filtra gaussowskiego, w odniesieniu do przebiegu bez filtra.	113
6.10	Prawdopodobieństwo detekcji w funkcji SNR obrazujące wpływ stosowania operacji morfologicznych i ich kolejności.	113
6.11	Przykładowe preambuły badanych sygnałów w wycinku spektrogramu o rozmiarze 64 na 64 piksele.	114
6.12	Architektura zastosowanej sieci wraz z wynikami klasyfikacji binarnej dla różnego rozmiaru regionu.	115
6.13	Podsumowanie wyników pracy metody dwuetapowej w odniesieniu do SNR: (a) dokładność klasyfikacji dla obu rozmiarów pola danych, (b) zestawienie charakterystyk wybranej sieci z technikami innych autorów i skutecznością detektora.	117
6.14	Ścieżka ewolucji sieci z rodziny YOLO [187].	119
6.15	Podsumowanie wyników działania modeli z rodziny YOLO dla wersji sieci o najniższej gęstości w odniesieniu do SNR.	121
6.16	Podsumowanie wyników działania modeli z rodziny YOLO dla wersji sieci o większej gęstości w odniesieniu do SNR.	121
6.17	Macierz pomyłek dla prototypu i algorytmu dwustopniowego w warunkach rzeczywistych dla różnych odległości nadajnika od odbiornika: (a) do 150 m, (b) do 350 m.	123

7.1	Charakterystyki promieniowania anten zastosowanych w symulacji zakłócania GPS L1.	127
7.2	Wyniki symulacji metodą śledzenia promieni określające parametr JSR dla sygnału GPS L1: (a,b) dla ścieżki <i>I</i> , (c,d) dla ścieżki <i>II</i> , (e,f) dla ścieżki <i>III</i> .128	
7.3	Schemat blokowy komercyjnego odbiornika GNSS.	130
7.4	Schemat blokowy stanowiska pomiarowego dla zakłócania sygnałów GNSS. 133	
7.5	Wpływ różnych fal zakłócających na parametry odbiornika podczas zakłócania konstelacji GPS L1.	134
7.6	Parametry odbiornika podczas zakłócania GNSS sinusoidalnym sygnałem przestrajającym w zakresie 1559 MHz do 1610 MHz z różnym czasem powtarzania.	136
7.7	Parametry odbiornika podczas zakłócania GNSS kombinowanym sygnałem przestrajającym.	137
7.8	Wyniki symulacji metodą śledzenia promieni określające parametr JSR dla sygnałów sterujących: (a,b) dla ścieżki <i>I</i> , (c,d) dla ścieżki <i>II</i> , (e,f) dla ścieżki <i>III</i>	139
7.9	Wyniki symulacji metodą śledzenia promieni określające parametr JSR dla sygnałów kierowania i kontroli dla drona operującego na wysokości 32 m. . 140	
7.10	Stanowisko eksperymentalne badania wpływu zakłócania na przepustowość w protokole 802.11n.	143
7.11	Zestawienie wyników badania wpływu różnych form zakłócania na szybkość transferu danych dla protokołu 802.11n: (a) wynik symulacji metody szumowej odniesiony do pomiarów, (b) zestawienie różnych czasów przestrajania fali sinusoidalnej.	143
7.12	Szkic planu pomiaru wpływu różnych technik zakłócających na bezzałogowe statki powietrzne.	144
7.13	Wyniki badań zasięgu zakłócania komercyjnych statków bezzałogowych operujących w pasmie ISM 2,4 GHz.	145

Spis tabel

5.1	Zakresy aktualnej pracy sieci 4G/LTE w Polsce.	94
6.1	Wyniki klasyfikacji binarnej dla różnych modeli oparte na metodzie analizy wycinka spektrogramu	115
6.2	Wyniki klasyfikacji binarnej oraz parametry zastosowanych sieci neuronowych wraz z czasem wykonywania obliczeń.	116
6.3	Parametry sieci z edycji YOLO 5 do 12.	120
7.1	Wartość parametru JSR w różnych opracowaniach	126
7.2	Systemy nawigacji satelitarnej wykorzystywane w popularnych modelach statków bezzałogowych.	135

Bibliografia

- [1] Jacek Chojnacki i Dominika Pasek. „Historia wykorzystania bezzałogowych statków powietrznych”. W: *Rocznik Bezpieczeństwa Międzynarodowego* 11.1 (2017), s. 174–189.
- [2] Bruno Martins, Arthur Holland i Andrea Silkoset. *Countering the Drone Threat Implications of C-UAS technology for Norway in an EU and NATO context*. Oslo: Peace Research Institute Oslo (PRIO), 2020. ISBN: 978-82-343-0074-5.
- [3] Anna Barlett. *Emerging Aviation Entrants: Unmanned Aircraft Systems and Advanced Air Mobility*. 2023. URL: https://www.faa.gov/data_research/aviation/aerospace_forecasts/unmanned_aircraft_systems.pdf (term. wiz. 15.02.2025).
- [4] Marcin Dżoń. *Liczba rejestracji operatorów SBSP oraz uzyskanych kompetencji pilotów BSP w roku 2024*. 2025. URL: <https://www.ulc.gov.pl/pl/statystyki-analizy/bezzalogowe-statki-powietrzne> (term. wiz. 15.02.2025).
- [5] Andrzej Fellner, Bogdan Mańka i Adam Mańka. „Analiza aktualnych metod detekcji bezzałogowych statków powietrznych (dronów)”. W: *TTS Technika Transportu Szybowego* 22.12 (2015), s. 484–488.
- [6] Samira Shackle. *The mystery of the Gatwick drone*. 2020. URL: <https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone> (term. wiz. 15.02.2025).
- [7] Paul Pradier. *Greenpeace intentionally crashes drone into French nuclear power plant to reveal security vulnerability*. 2018. URL: <https://abcnews.go.com/International/greenpeace-intentionally-crashes-drone-french-nuclear-power-plant/story?id=56343027> (term. wiz. 15.02.2025).
- [8] Tim Wright. *How Many Drones Are Smuggling Drugs Across the U.S. Southern Border?* 2020. URL: <https://www.smithsonianmag.com/air-space-magazine/narcodrones-180974934/> (term. wiz. 15.02.2025).
- [9] Thomas Pledger. „The Role of Drones in Future Terrorist Attacks”. W: *Association of the United States Army* 137.2 (2021), s. 1–10.

- [10] Agnieszka Fortońska. „Drone Harassment Case Before the Polish Supreme Court”. W: *Air and Space Law* 48.6 (2023), s. 611–616.
- [11] Jędrzej Łukasiewicz. „Bezzałogowe statki powietrzne jako źródło zagrożeń infrastruktury zaopatrzenia państw w energię elektryczną oraz proponowane metody ochrony tej infrastruktury”. W: *Terroryzm: studia, analizy, prewencja* 1.1 (2022), s. 90–122.
- [12] Tadeusz Zieliński. „Zagrożenia i przeciwdziałanie bezzałogowym statkom powietrznym w ochronie portów lotniczych”. W: *Rocznik Bezpieczeństwa Morskiego XVI* (2022), s. 1–20.
- [13] Jing Jing Yang, Dezhang Chen, Hao Tang, Jiang Yu i Ming Huang. „Cooperative compressed spectrum sensing model for regional radio monitoring”. W: *2014 XXXIth URSI General Assembly and Scientific Symposium (URSI GASS)*. 2014, s. 1–4.
- [14] Paweł Skokowski, Krzysztof Malon i Jerzy Łopatka. „Building the Electromagnetic Situation Awareness in MANET Cognitive Radio Networks for Urban Areas”. W: *Sensors* 22.3 (2022), s. 716.
- [15] Przemysław Flak. „Drone Detection Sensor With Continuous 2.4 GHz ISM Band Coverage Based on Cost-Effective SDR Platform”. W: *IEEE Access* 9 (2021), s. 114574–114586.
- [16] Przemysław Flak. „Hardware-Accelerated Real-Time Spectrum Analyzer With a Broadband Fast Sweep Feature Based on the Cost-Effective SDR Platform”. W: *IEEE Access* 10 (2022), s. 110934–110946.
- [17] Andrzej Świerniak i Jolanta Krystek. *Automatyzacja procesów dyskretnych. Teoria i zastosowania*. Gliwice: Wydawnictwo Politechniki Śląskiej, 2022. ISBN: 978-83-7880-854-1.
- [18] Przemysław Flak i Roman Czyba. „RF Drone Detection System Based on a Distributed Sensor Grid With Remote Hardware-Accelerated Signal Processing”. W: *IEEE Access* 11 (2023), s. 138759–138772.
- [19] Alessandro Brighente, Mauro Conti, Giacomo Peruzzi i Alessandro Pozzebon. „Anti-Drone Audio Surveillance Sentinel via Embedded Machine Learning”. W: *2023 IEEE Sensors Applications Symposium (SAS)*. 2023, s. 1–6.
- [20] Daniel Kadyrov, Alexander Sedunov, Nikolay Sedunov, Alexander Sutin, Hady Salloum i Sergey Tsyuryupa. „Improvements to the Stevens drone acoustic detection system”. W: *Proceedings of Meetings on Acoustics* 46.1 (2022), s. 045001.

-
- [21] Jian Fang, Yaowen Li, Philip N. Ji i Ting Wang. „Drone Detection and Localization Using Enhanced Fiber-Optic Acoustic Sensor and Distributed Acoustic Sensing Technology”. W: *Journal of Lightwave Technology* 41.3 (2023), s. 822–831.
- [22] Vinicius G. Goecks, Grayson Woods i John Valasek. „Combining visible and infrared spectrum imagery using machine learning for small unmanned aerial system detection”. W: *Automatic Target Recognition XXX*. 2020, s. 113940.
- [23] Md Shovon, Rohit Gopalan i Benjamin Campbell. „A comparative analysis of deep learning algorithms for optical drone detection”. W: *Fifteenth International Conference on Machine Vision (ICMV 2022)*. 2023, s. 1270104.
- [24] Denis Ojdanić, Andreas Sinn, Christopher Naverschnigg i Georg Schitter. „Feasibility Analysis of Optical UAV Detection Over Long Distances Using Robotic Telescopes”. W: *IEEE Transactions on Aerospace and Electronic Systems* 59.5 (2023), s. 5148–5157.
- [25] Bashar I. Ahmad, Colin Rogers, Stephen Harman, Holly Dale, Mohammed Jahangir, Michael Antoniou, Chris Baker, Mike Newman i Francesco Fioranelli. „A Review of Automatic Classification of Drones Using Radar: Key Considerations, Performance Evaluation, and Prospects”. W: *IEEE Aerospace and Electronic Systems Magazine* 39.2 (2024), s. 18–33.
- [26] Jun Yan, Huiping Hu, Jiangkun Gong, Deyong Kong i Deren Li. „Exploring Radar Micro-Doppler Signatures for Recognition of Drone Types”. W: *Drones* 7.4 (2023), s. 280.
- [27] Martin Ummenhofer, Louis Cesbron Lavau, Diego Cristallini i Daniel O’Hagan. „UAV Micro-Doppler Signature Analysis Using DVB-S Based Passive Radar”. W: *2020 IEEE International Radar Conference (RADAR)*. 2020, s. 1007–1012.
- [28] Peter John Rodrigo, Henning Larsen i Christian Pedersen. „CW coherent detection lidar for micro-Doppler sensing and raster-scan imaging of drones”. W: *Optics Express* 31 (2023), s. 7398–7412.
- [29] Tasnim Azad Abir, Endrowednes Kuantama, Richard Han, Judith Dawes, Rich Mildren i Phuc Nguyen. „Towards Robust Lidar-based 3D Detection and Tracking of UAVs”. W: *Proceedings of the Ninth Workshop on Micro Aerial Vehicle Networks, Systems, and Applications*. 2023, s. 1–7.
- [30] Konstantinos Paschalidis, Oleg Yakimenko i Roberto Cristi. „Feasibility of using 360 LiDAR in C-sUAS Missions”. W: *2022 IEEE 17th International Conference on Control and Automation (ICCA)*. 2022, s. 172–179.
- [31] Igor Bisio, Chiara Garibotto, Fabio Lavagetto, Andrea Sciarrone i Sandro Zappatore. „Blind Detection: Advanced Techniques for WiFi-Based Drone Surveillance”. W: *IEEE Transactions on Vehicular Technology* 68.1 (2019), s. 938–946.

- [32] Nico Schiller, Merlin Chlosta, Moritz Schloegel, Nils Bars, Thorsten Eisenhofer, Tobias Scharnowski, Felix Domke, Lea Schönherr i Thorsten Holz. „Drone Security and the Mysterious Case of DJI’s DroneID”. W: *Network and Distributed System Security Symposium (NDSS)*. 2023.
- [33] Martins Ezuma, Fatih Erden, Chethan Kumar Anjinappa, Ozgur Ozdemir i Ismail Guvenc. „Detection and Classification of UAVs Using RF Fingerprints in the Presence of Wi-Fi and Bluetooth Interference”. W: *IEEE Open Journal of the Communications Society* 1 (2020), s. 60–76.
- [34] Batuhan Kaplan, İbrahim Kahraman, Ali Görçin, Hakan Ali Çırpan i Ali Rıza Ekti. „Measurement based FHSS-type Drone Controller Detection at 2.4GHz: An STFT Approach”. W: *2020 IEEE 91st Vehicular Technology Conference (VTC2020-Spring)*. 2020, s. 1–6.
- [35] Florin Chiper, Alexandru Martian, Calin Vladeanu, Marghescu Ion, Razvan Cra-ciunescu i Octavian Fratu. „Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution”. W: *Sensors* 22 (lut. 2022), s. 1453.
- [36] Oscar Javier Montañez, Marco Javier Suarez i Eduardo Avendano Fernandez. „Ap-plication of Data Sensor Fusion Using Extended Kalman Filter Algorithm for Iden-tification and Tracking of Moving Targets from LiDAR–Radar Data”. W: *Remote Sensing* 15.13 (2023), s. 3396.
- [37] Mohammed Aledhari, Rehman Razzak, Reza M. Parizi i Gautam Srivastava. „Sensor Fusion for Drone Detection”. W: *2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)*. 2021, s. 1–7.
- [38] Varun Mehta, Fardad Dadboud, Miodrag Bolic i Iraj Mantegh. „A Deep Learning Approach for Drone Detection and Classification Using Radar and Camera Sensor Fusion”. W: *2023 IEEE Sensors Applications Symposium (SAS)*. 2023, s. 01–06.
- [39] Pengfei Liu. „Research on Detection and Attack Strategy Against Swarm of Drones”. W: *2023 IEEE 11th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)*. 2023, s. 1648–1653.
- [40] Mia Stevens i Ella Atkins. „Geofencing in Immediate Reaches Airspace for Unman-ned Aircraft System Traffic Management”. W: *AIAA Sci Tech Forum*. Sty. 2018, s. 1–11.
- [41] Jennifer Ambrose. *Executive Summary Final Rule on Remote Identification of Unmanned Aircraft (Part 89)*. 2020. URL: https://www.faa.gov/sites/faa.gov/files/uas/getting_started/remote_id/RemoteID_Executive_Summary.pdf (term. wiz. 19.02.2025).

-
- [42] Saulius Rudys, Andrius Laučys, Paulius Ragulis, Rimvydas Aleksiejūnas, Karolis Stankevičius, Martynas Kinka, Matas Razgūnas, Domantas Bručas, Dainius Udris i Raimondas Pomarnacki. „Hostile UAV Detection and Neutralization Using a UAV System”. W: *Drones* 6.9 (2022), s. 250.
- [43] Kin Low. „An initial parametric study of weight and energy thresholds for falling unmanned aerial vehicles (UAVs)”. W: *2017 Workshop on Research, Education and Development of Unmanned Aerial Systems (RED-UAS)*. 2017, s. 240–245.
- [44] Evan Ackerman. *Dutch Police Training Eagles to Take Down Drones*. 2016. URL: <https://spectrum.ieee.org/dutch-police-training-eagles-to-take-down-drones> (term. wiz. 19.02.2025).
- [45] Julian Rothe, Michael Strohmeier i Sergio Montenegro. „A concept for catching drones with a net carried by cooperative UAVs”. W: *2019 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)*. 2019, s. 126–132.
- [46] Eric Horton i Prakash Ranganathan. „Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter”. W: *The Journal of Global Positioning Systems* 16.9 (2018).
- [47] Lester Faria, Caio Silvestre i Marcelino Correia. „GPS-Dependent Systems: Vulnerabilities to Electromagnetic Attacks”. W: *Journal of Aerospace Technology and Management* 8.4 (2016), s. 423–430.
- [48] Fang Ye, Hongbo Tian i Fei Che. „CW interference effects on the performance of GPS receivers”. W: *2017 Progress in Electromagnetics Research Symposium - Fall (PIERS - FALL)*. 2017, s. 66–72.
- [49] Renato Ferreira, João Gaspar, Nuno Souto i Pedro Sebastião. „Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms”. W: *2018 Global Wireless Summit (GWS)*. 2018, s. 27–32.
- [50] Ondřej Šimon i Tomáš Götthans. „A Survey on the Use of Deep Learning Techniques for UAV Jamming and Deception”. W: *Electronics* 11.19 (2022), s. 3025.
- [51] Philip E. Ross. „Economics Drives a Ray-Gun Resurgence: Lasers, Cheaper by the Shot, Should Work Well Against Drones and Cruise Missiles”. W: *IEEE Spectrum* 60.1 (2023), s. 40–41.
- [52] Longwen Liao, Xiaoliang Huang i Fengyu Xie. „Development Status and Operation Analysis of Laser Weapon in Anti-Drone Warfare”. W: *2023 IEEE International Conference on Unmanned Systems (ICUS)*. 2023, s. 305–310.

- [53] Sun-Hong Min, Hoechun Jung, Ohjoon Kwon, Matlabjon Sattorov, Seontae Kim, Seung-Hyuk Park, Dongpyo Hong, Seonmyeong Kim, Chawon Park, Bong Hwan Hong, Ilsung Cho, Sukhwal Ma, Minho Kim, Young Joon Yoo, Sang Yoon Park i Gun-Sik Park. „Analysis of Electromagnetic Pulse Effects Under High-Power Microwave Sources”. W: *IEEE Access* 9.1 (2021), s. 136775–136791.
- [54] Stanisław Czeszejko i Józef Janczak. „Militarne aspekty środowiska elektronicznego: próba rewizji istniejącej terminologii”. W: *Zeszyty Naukowe AON* 98.1 (2015), s. 76–103.
- [55] Leopold Ciborowski. *Walka informacyjna*. Toruń: Europejskie Centrum Edukacyjne, 2002. ISBN: 8373224084.
- [56] Rafał Kopeć i Maciej Kulczycki. *Vademecum Bezpieczeństwa Informacyjnego*. 2020. URL: <https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/walka-elektroniczna/> (term. wiz. 15.02.2025).
- [57] Rafał Kopeć. *Vademecum Bezpieczeństwa Informacyjnego*. 2020. URL: <https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/walka-radioelektroniczna/> (term. wiz. 15.02.2025).
- [58] Tomasz P. Zieliński. *Cyfrowe przetwarzanie sygnałów*. Warszawa: Wydawnictwa Komunikacji i Łączności, 2007. ISBN: 978-83-206-1866-2.
- [59] Jerzy Szabatin. *Podstawy teorii sygnałów*. Warszawa: Wydawnictwa Komunikacji i Łączności, 2000. ISBN: 83-206-1331-0.
- [60] M. Bugaj i M. Wnuk. „Modelowanie rozchodzenia się fal elektromagnetycznych w warunkach idealnych i rzeczywistych”. W: *Przegląd Elektrotechniczny* 90.7 (2014), s. 152–155.
- [61] Simon R. Saunders i Alejandro Aragón-Zavala. *Antennas and Propagation for Wireless Communication Systems 3e*. Chichester: John Wiley i Sons, Ltd, 2024. ISBN: 9781119332206.
- [62] LalChand Godara. *Handbook of Antennas in Wireless Communications*. London: London CRC Press, 2002. ISBN: 0-8493-0124-6.
- [63] Baohai Yang, Quanhui Ren, Haisheng Li i Junkang Song. „A Low-Signal-to-Noise Ratio Estimation Algorithm for Multipath Channels”. W: *Ingénierie des systèmes d'information* 25 (maj 2020), s. 253–258.
- [64] Fred Harris i Chris Dick. „SNR estimation techniques for low SNR signals”. W: *The 15th International Symposium on Wireless Personal Multimedia Communications*. 2012, s. 276–280.

-
- [65] Hongjian Sun, Arumugam Nallanathan, Cheng-Xiang Wang i Yunfei Chen. „Wide-band spectrum sensing for cognitive radio networks: a survey”. W: *IEEE Wireless Communications* 20.2 (2013), s. 74–81.
- [66] Youness Arjouni i Naima Kaabouch. „A Comprehensive Survey on Spectrum Sensing in Cognitive Radio Networks: Recent Advances, New Challenges, and Future Research Directions”. W: *Sensors* 19.1 (2019), s. 1–32.
- [67] Runze Wan, Lixin Ding, Naixue Xiong, Wanneng Shu i Li Yang. „Dynamic dual threshold cooperative spectrum sensing for cognitive radio under noise power uncertainty”. W: *Hum.-Centric Comput. Inf. Sci.* 9.1 (2019), s. 1–21.
- [68] Adeiza Onumanyi, Adnan Abu-Mahfouz i Gerhard Hancke. „Amplitude quantization method for autonomous threshold estimation in self-reconfigurable cognitive radio systems”. W: *Physical Communication* 44.2 (2021), s. 1–18.
- [69] Nobuyuki Otsu. „A Threshold Selection Method from Gray-Level Histograms”. W: *IEEE Transactions on Systems, Man, and Cybernetics* 9.1 (1979), s. 62–66.
- [70] Sudhamani Chilakala, Ashutosh Saxena i Vunnava Aswini. „Improved Detection Performance of Energy Detection Based Spectrum Sensing in Cognitive Radio Networks”. W: *International Journal of Sensors, Wireless Communications and Control* 11.9 (2021), s. 957–962.
- [71] Shanshan Yu, Ju Liu, Jing Wang i Inam Ullah. „Adaptive Double-Threshold Cooperative Spectrum Sensing Algorithm Based on History Energy Detection”. W: *Wireless Communications and Mobile Computing* 2020.1 (2020), s. 4794136.
- [72] Muhammad Umair Muzaffar i Rula Sharqi. „A review of spectrum sensing in modern cognitive radio networks”. W: *Telecommunication Systems* 85 (list. 2023), s. 1–17.
- [73] Tevfik Yucek i Huseyin Arslan. „A survey of spectrum sensing algorithms for cognitive radio applications”. W: *IEEE Communications Surveys and Tutorials* 11.1 (2009), s. 116–130.
- [74] Haiyun Tang. „Some physical layer issues of wide-band cognitive radio systems”. W: *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.* 2005, s. 151–159.
- [75] Varsha Saxena i S. J. Bsaha. „A Survey of Various Spectrum Sensing Techniques in Cognitive Radio Networks: Non Cooperative Systems”. W: *International Journal of Electronics Communication and Computer Engineering* 4.3 (2013), s. 857–862.

- [76] Arun Kumar, J. Venkatesh, Nishant Gaur, Mohammed H. Alsharif, Peerapong Uthansakul i Monthippa Uthansakul. „Cyclostationary and energy detection spectrum sensing beyond 5G waveforms”. W: *Electronic Research Archive* 31.6 (2023), s. 3400–3416.
- [77] Akin Özkaner i Yetkin Akça. „Mini/Micro UAV detection in the presence of ISM or spurious signals and an experimental application on an SDR”. W: *Engineering Science and Technology, an International Journal* 49.1 (2024), s. 101591.
- [78] Ewa Wędrawska. „Wykorzystanie entropii Shannona i jej uogólnień do badania rozkładu prawdopodobieństwa zmiennej losowej dyskretnej”. W: *Przegląd Statystyczny* 57.z. 4 (2010), s. 39–53.
- [79] Ángel G. Andrade Guillermo Prieto i Daniela M. Martínez. „Numerical Analysis of Histogram-based Estimation Techniques for Entropy-based Spectrum Sensing”. W: *IETE Technical Review* 37.1 (2020), s. 91–97.
- [80] Claude Elwood Shannon. „A mathematical theory of communication”. W: *SIG-MOBILE Mobile Computing and Communications Review* 5.1 (2001), s. 3–55.
- [81] Y. Zhang, Q. Zhang i S. Wu. „Entropy-based robust spectrum sensing in cognitive radio”. W: *IET Communications* 4.4 (2010), s. 428–436.
- [82] Yi-Yong Zhu i Yong-Gang Zhu. „The simulation study of entropy-based signal detector over fading channel”. W: *2012 International Conference on Wireless Communications and Signal Processing (WCSP)*. 2012, s. 1–5.
- [83] Mustefa Badri Usman, Ram Sewak Singh, S Rajkumar i Jiafeng Zhou. „Stage Spectrum Sensing Technique for Cognitive Radio Network Using Energy and Entropy Detection”. W: *Wireless Power Transfer* 2022.8 (2022), s. 1–10.
- [84] G. Vaidehi, Namburu Swetha i Panyam Narahari Sastry. „Entropy based Spectrum Sensing in Cognitive Radio Networks”. W: *International Journal of Advanced Research Computer and Communication Engineering* 4.11 (2015), s. 39–43.
- [85] Ernesto Muñoz, Luis Pedraza i Cesar Hernández. „Rényi Entropy-Based Spectrum Sensing in Mobile Cognitive Radio Networks Using Software Defined Radio”. W: *Entropy* 22.6 (2020), s. 1–15.
- [86] Aleksandra Król-Nowak. *Podstawy uczenia maszynowego*. Kraków: Wydawnictwa AGH, 2022. ISBN: 978-83-67427-05-0.
- [87] Andriy Burkov. *The Hundred-Page Machine Learning Book*. Onilne: Burkov, Andriy, 2019. ISBN: 978-19-99579-51-7.
- [88] Bohdan Macukow. *Sieci neuronowe, historia badań i podstawowe modele*. Warszawa: Oficyna Wydawnicza Politechniki Warszawskiej, 2020. ISBN: 978-83-8156-175-4.

-
- [89] Waldemar Scheffs. „Atrybuty walki radioelektronicznej w sztuce wojennej”. W: *Przegląd Geopolityczny* 49 (2024), s. 126–149.
- [90] David Adamy. *EW 101: A First Course in Electronic Warfare*. London: Artech House, 2001. ISBN: 1-58053-169-5.
- [91] Marc Lichtman, Jeffrey D. Poston, SaiDhiraj Amuru, Chowdhury Shahriar, T. Charles Clancy, R. Michael Buehrer i Jeffrey H. Reed. „A communications jamming taxonomy”. W: *IEEE Security and Privacy* 14.1 (2016), s. 47–54.
- [92] Joseph Angelo. *Measuring GNSS Signal Strength*. 2010. URL: <https://insidegnss.com/measuring-gnss-signal-strength/> (term. wiz. 21.04.2025).
- [93] Mujahid Mohsin Muhammad Farhan Shahid Khuram Mehmood. *Taxonomy of Physical Layer Jamming Techniques and Strategies for Security Enhancement in Wireless Communication : A Comprehensive Survey*. 2024. URL: <https://www.techrxiv.org/users/690897/articles/1215995-taxonomy-of-physical-layer-jamming-techniques-and-strategies-for-security-enhancement-in-wireless-communication-a-comprehensive-survey?commit=587a0875de534bb4ba9f5e6c0ebeab57d9162528> (term. wiz. 21.04.2025).
- [94] EASA. *Open Category-Low Risk-Civil Drones*. 2024. URL: <https://www.easa.europa.eu/en/domains/drones-air-mobility/operating-drone/open-category-low-risk-civil-drones#group-easa-downloads> (term. wiz. 19.02.2025).
- [95] DJI. *Fly Safe, DJI AirSense*. 2025. URL: <https://www.dji.com/pl/flysafe/airsense> (term. wiz. 19.02.2025).
- [96] DJI. *Aeroscope*. 2025. URL: <https://www.dji.com/pl/aeroscope> (term. wiz. 19.02.2025).
- [97] DJI ViewPoints Team. *DJI's GEO System Is An Education - Not Enforcement - Tool*. 2025. URL: <https://viewpoints.dji.com/blog/djis-geo-system-is-an-education-not-enforcement-tool> (term. wiz. 19.02.2025).
- [98] David Rozenbeek. *Evaluation of Drone Neutralization Methods using Radio Jamming and Spoofing Techniques*. 2020. URL: <https://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-279557> (term. wiz. 19.02.2025).
- [99] Texas Instruments. *Sub-1GHz: Robustness and Long Range*. 2013. URL: https://www.ti.com/download/trng/multimedia/dsp/OLT/OLT313007_p0.pdf (term. wiz. 19.02.2025).
- [100] Sanjoy Basak, Sreeraj Rajendran, Sofie Pollin i Bart Scheers. „Spectrum Prediction for Protocol-Aware RF Jamming”. W: *IEEE Transactions on Cognitive Communications and Networking* 10.2 (2024), s. 363–373.

- [101] Driss Aouladhadj, Ettien Kpre, Virginie Deniau, Aymane Kharchouf, Christophe Gransart i Christophe Gaquière. „Drone Detection and Tracking Using RF Identification Signals”. W: *Sensors* 23.17 (2023), s. 1–24.
- [102] Matthew S. Gast. *802.11 Wireless Networks: The Definitive Guide*. Sebastopol: O’Reilly Media, 2003. ISBN: 0596100523.
- [103] TAOGLAS. *GNSS Constellations, Radio Frequencies and Signals*. 2025. URL: <https://www.calian.com/advanced-technologies/gnss/information-support/gnss-constellations-radio-frequencies-and-signals/> (term. wiz. 19.02.2025).
- [104] Kais Belwafi, Ruba Alkadi, Sultan A. Alameri, Hussam Al Hamadi i Abdulhadi Shoufan. „Unmanned Aerial Vehicles’ Remote Identification: A Tutorial and Survey”. W: *IEEE Access* 10 (2022), s. 87577–87601.
- [105] Sean Hollister. *The drone pilot who took out an LA firefighting plane pleads guilty to escape prison*. 2025. URL: <https://www.theverge.com/news/604527/drone-crashed-into-la-wildfire-plane-plea-deal> (term. wiz. 19.02.2025).
- [106] University of Dayton Research Institute. *When Planes And Drones Collide*. 2019. URL: <https://udayton.edu/blogs/momentum/2018/11/udri-drone-test.php> (term. wiz. 19.02.2025).
- [107] Mart Keizer, Savio Sciancalepore i Gabriele Oliveri. „GhostBuster: Detecting Misbehaving Remote ID-Enabled Drones”. W: *2024 IEEE 21st Consumer Communications and Networking Conference (CCNC)*. 2024, s. 324–332.
- [108] Abhishek Phadke, Josh Boyd, F. Medrano i Michael Starek. „Navigating the skies: examining the FAA’s remote identification rule for unmanned aircraft systems”. W: *Drone Systems and Applications* 11.08 (2023), s. 1–4.
- [109] Pietro Tedeschi, Fatima Ali Al Nuaimi, Ali Ismail Awad i Enrico Natalizio. „Privacy-Aware Remote Identification for Unmanned Aerial Vehicles: Current Solutions, Potential Threats, and Future Directions”. W: *IEEE Transactions on Industrial Informatics* 20.2 (2024), s. 1069–1080.
- [110] Guang Yang, Xiufang Shi, Li Feng, Shibo He, Zhiguo Shi i Jiming Chen. „CEDAR: A Cost-Effective Crowdsensing System for Detecting and Localizing Drones”. W: *IEEE Transactions on Mobile Computing* 19.9 (2020), s. 2028–2043.
- [111] Simon Birnbach, Richard Baker i Ivan Martinovic. „Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones”. W: *Proceedings of the 24th Annual Network and Distributed System Security Symposium (NDSS)*. 2017, s. 127–132.

- [112] Ashok Vardhan Raja. *Uncover the Power of Multipath : Detecting NLOS Drones Using Low-Cost WiFi Devices*. 2019. URL: <https://commons.erau.edu/edt/441> (term. wiz. 01.04.2021).
- [113] Amir Alipour-Fanid, Monireh Dabaghchian, Ning Wang, Pu Wang, Liang Zhao i Kai Zeng. „Machine Learning-Based Delay-Aware UAV Detection and Operation Mode Identification Over Encrypted Wi-Fi Traffic”. W: *IEEE Transactions on Information Forensics and Security* 15.1 (2020), s. 2346–2360.
- [114] Derry Pratama, Jaegeun Moon, Agus Mahardika Ari Laksmo, Dongwook Yun, Muhammad Iqbal, Byeonguk Jeong, Jang Hyun Ji i Howon Kim. „Behind The Wings: The Case of Reverse Engineering and Drone Hijacking in DJI Enhanced Wi-Fi Protocol”. W: *2024 International Conference on Platform Technology and Service (PlatCon)*. 2024, s. 127–132.
- [115] Nasim Soltani, Guillem Reus-Muns, Batool Salehi, Jennifer Dy, Stratis Ioannidis i Kaushik Chowdhury. „RF Fingerprinting Unmanned Aerial Vehicles With Non-Standard Transmitter Waveforms”. W: *IEEE Transactions on Vehicular Technology* 69.12 (2020), s. 15518–15531.
- [116] S. Kunze i B. Saha. „Drone Classification with a Convolutional Neural Network Applied to Raw IQ Data”. W: *2022 3rd URSI Atlantic and Asia Pacific Radio Science Meeting (AT-AP-RASC)*. 2022, s. 1–4.
- [117] Sara Al-Emadi i Felwa Al-Senaid. „Drone Detection Approach Based on Radio-Frequency Using Convolutional Neural Network”. W: *2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT)*. 2020, s. 29–34.
- [118] Thien Huynh-The, Quoc-Viet Pham, Toan-Van Nguyen, Daniel Benevides Da Costa i Dong-Seong Kim. „RF-UAVNet: High-Performance Convolutional Network for RF-Based Drone Surveillance Systems”. W: *IEEE Access* 10.5 (2022), s. 49696–49707.
- [119] Syed Samiul Alam, Arbil Chakma, Md Habibur Rahman, Raihan Bin Mofidul, Md Morshed Alam, Ida Bagus Krishna Yoga Utama i Yeong Min Jang. „RF-Enabled Deep-Learning-Assisted Drone Detection and Identification: An End-to-End Approach”. W: *Sensors* 23.9 (2023), s. 1–18.
- [120] Hanshuo Zhang, Tao Li, Nan Su, Dishan Wei, Yongzhao Li i Zhijin Wen. „Drone Identification Based on Normalized Cyclic Prefix Correlation Spectrum”. W: *IEEE Transactions on Cognitive Communications and Networking* 10.4 (2024), s. 1241–1252.

- [121] Mohammad F. Al-Sa'd, Abdulla Al-Ali, Amr Mohamed, Tamer Khattab i Aiman Erbad. „RF-based drone detection and identification using deep learning approaches: An initiative towards a large open source drone database”. W: *Future Generation Computer Systems* 100 (2019), s. 86–97.
- [122] Ibrahim Nemer, Tarek Sheltami, Irfan Ahmad, Ansar Ul-Haque Yasar i Mohammad A. R. Abdeen. „RF-Based UAV Detection and Identification Using Hierarchical Learning Approach”. W: *Sensors* 21.6 (2021), s. 1–23.
- [123] Yongguang Mo, Jianjun Huang i Gongbin Qian. „Deep Learning Approach to UAV Detection and Classification by Using Compressively Sensed RF Signal”. W: *Sensors* 22.8 (2022), s. 1–15.
- [124] Hao Zhang, Conghui Cao, Lingwei Xu i T. Aaron Gulliver. „A UAV Detection Algorithm Based on an Artificial Neural Network”. W: *IEEE Access* 6.5 (2018), s. 24720–24728.
- [125] Ming Zuo, Shuguo Xie, Xian Zhang i Meiling Yang. „Recognition of UAV Video Signal Using RF Fingerprints in the Presence of WiFi Interference”. W: *IEEE Access* 9.6 (2021), s. 88844–88851.
- [126] Sanjoy Basak, Sreeraj Rajendran, Sofie Pollin i Bart Scheers. „Drone classification from RF fingerprints using deep residual nets”. W: *2021 International Conference on COMmunication Systems and NETworkS (COMSNETS)*. 2021, s. 548–555.
- [127] Chengtao Xu, Bowen Chen, Yongxin Liu, Fengyu He i Houbing Song. „RF Fingerprint Measurement For Detecting Multiple Amateur Drones Based on STFT and Feature Reduction”. W: *2020 Integrated Communications Navigation and Surveillance Conference (ICNS)*. 2020, 4G1-1-4G1–7.
- [128] Chaozheng Xue, Tao Li, Yongzhao Li, Yuhan Ruan i Rui Zhang. „Radio Frequency Identification for Drones Using Spectrogram and CNN”. W: *GLOBECOM 2022 - 2022 IEEE Global Communications Conference*. 2022, s. 4564–4569.
- [129] Ender Ozturk, Fatih Erden i Ismail Guvenc. „RF-based low-SNR classification of UAVs using convolutional neural networks”. W: *ITU Journal on Future and Evolving Technologies* 2.07 (2021), s. 39–52.
- [130] Fares Mehouchi, Qingjie Yang, Juan Galvis Sarria, Santiago Morales, Milosch Meriac, Felix Vega i Chaouki Kasmi. *Detection of UAVs Based on Spectrum Monitoring and Deep Learning in Negative SNR Conditions*. 2022. URL: <https://api.semanticscholar.org/CorpusID:248456600> (term. wiz. 02.04.2024).
- [131] Hanshuo Zhang, Tao Li, Yongzhao Li i Zhijin Wen. „Virtual electromagnetic environment modeling based data augmentation for drone signal identification”. W: *Journal of Information and Intelligence* 1.4 (2023), s. 308–320.

-
- [132] Stefan Glüge, Matthias Nyfeler, Ahmad Aghaebrahimian, Nicola Ramagnano i Christof Schüpbach. „Robust Low-Cost Drone Detection and Classification Using Convolutional Neural Networks in Low SNR Environments”. W: *IEEE Journal of Radio Frequency Identification* 8 (2024), s. 821–830.
- [133] Karen Simonyan i Andrew Zisserman. „Very Deep Convolutional Networks for Large-Scale Image Recognition”. W: *International Conference on Learning Representations*. 2015, s. 1–14.
- [134] N. Norhashim, N. L. Mohd Kamal, Z. Sahwee, S. Ahmad Shah i D. Sathyamoorthy. „The Effects of Jamming on Global Positioning System (GPS) Accuracy for Unmanned Aerial Vehicles (UAVs)”. W: *2022 International Conference on Computer and Drone Applications (IConDA)*. 2022, s. 18–22.
- [135] Nurhakimah Norhashim, Nadhiya Liyana Mohd Kamal, Zulhilmy Sahwee, Shahrul Ahmad Shah, Nur Afiqah Alfian i Dinesh Sathyamoorthy. „GPS Jamming Impact on UAV Performance in Outdoor Environments”. W: *Defence Technical Bulletin* 17.1 (2024), s. 90–97.
- [136] Renato Ferreira, João Gaspar, Pedro Sebastião i Nuno Souto. „Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms”. W: *Wireless Personal Communications* 115.4 (2020), s. 2705–2727.
- [137] Younes Zidane, José Silvestre Silva i Gonçalo Tavares. „Jamming and Spoofing Techniques for Drone Neutralization: An Experimental Study”. W: *Drones* 8.12 (2024), s. 1–18.
- [138] Ahmad Danial Bin Abdul Rahman, Kamaruddin Abdul Ghani, Nor Hisham H Khamis i Abd Rahim Mat Sidek. „Unmanned Aerial Vehicle (UAV) GPS Jamming Test by using Software Defined Radio (SDR) platform”. W: *Journal of Physics: Conference Series* 1793.1 (2021), s. 012060.
- [139] Tomáš Morong, Pavel Puričér i Pavel Kovář. „Study of the GNSS Jamming in Real Environment”. W: *International Journal of Electronics and Telecommunications* 65.1 (2019), s. 65–70.
- [140] Nicolas Miguel, Yu-Hsuan Chen, Sherman Lo, Todd Walter i Dennis Akos. „Stress Testing of a Low-Cost GNSS RFI Monitor”. W: *35th International Technical Meeting of the Satellite Division of The Institute of Navigation*. 2022, s. 3463–3478.
- [141] S Shashank, Vinay B. Narayane, Paresh Saxena i Ashutosh Baheti. „Multiband Jamming Waveform Design for Advanced GNSS Receivers and UAVs”. W: *2024 IEEE Microwaves, Antennas, and Propagation Conference (MAPCON)*. 2024, s. 1–5.

- [142] Harshad Sathaye, Martin Strohmeier, Vincent Lenders i Aanjhan Ranganathan. „An Experimental Study of GPS Spoofing and Takeover Attacks on UAVs”. W: *31st USENIX Security Symposium (USENIX Security 22)*. 2022, s. 3503–3520.
- [143] Karel Pärlin, Muhammad Mahtab Alam i Yannick Le Moullec. „Jamming of UAV remote control systems using software defined radio”. W: *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. 2018, s. 1–6.
- [144] Jaakko Marin, Mikko Heino, Joni Saikanmäki, Miikka Mäenpää, Antti-Pekka Saarinen i Taneli Riihonen. „Perfecting Jamming Signals Against RC Systems: An Experimental Case Study on FHSS with GFSK”. W: *2020 IEEE 31st Annual International Symposium on Personal, Indoor and Mobile Radio Communications*. 2020, s. 1–5.
- [145] Pascal Thiele, Laura Bernadó, David Löschenbrand, Benjamin Rainer, Christoph Sulzbachner, Maria Leitner i Thomas Zemen. „Machine Learning Based Prediction of Frequency Hopping Spread Spectrum Signals”. W: *2023 IEEE 34th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*. 2023, s. 1–6.
- [146] Angsom Ataklity Tesfay, Driss Aouladhadj, Virginie Deniau, Christophe Gransart, Mickael Dufour i Patrick Sondi. „Smart Jamming: Deep Learning-Based UAVs Neutralization System”. W: *2024 International Symposium on Electromagnetic Compatibility – EMC Europe*. 2024, s. 380–384.
- [147] Ilkka Harjula, Jarno Pinola i Jarmo Prokkola. „Performance of IEEE 802.11 based WLAN devices under various jamming signals”. W: *2011 - MILCOM 2011 Military Communications Conference*. 2011, s. 2129–2135.
- [148] Mohammed RABIAI, Mohammed Raouf SENOUCI, Abdelkader SENOUCI, Krishna BUSAWON i Laurent DALA. „A hardware solution to overcome the bandwidth limitation of drone jamming platforms”. W: *12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*. 2020, s. 1–4.
- [149] Feten Slimeni i Tijeni Dalleji. „RF-based mini-Drone Detection, Identification and Jamming in No Fly Zones using Software Defined Radio”. W: *Computational Collective Intelligence*. 2022, s. 791–798.
- [150] Florin-Lucian Chipper, Alexandru Martian, Calin Vladeanu, Ion Marghescu, Razvan Craciunescu i Octavian Fratu. „Drone Detection and Defense Systems: Survey and a Software-Defined Radio-Based Solution”. W: *Sensors* 22.4 (2022), s. 1–27.

- [151] Jan Farlik, Miroslav Kratky i Josef Casar. „Detectability and jamming of small UAVs by commercially available low-cost means”. W: *2016 International Conference on Communications (COMM)*. 2016, s. 327–330.
- [152] Mario Andrés Ramos, Raul Camacho, Paola Andrea Buitrago, Robert David Urda i Julio Pastor Restrepo. „Software Defined Radio, a perspective from education”. W: *Frontiers in Education* 8.1 (2024).
- [153] Lime Microsystems Ltd. *SDR*. 2025. URL: <https://limemicro.com/> (term. wiz. 02.05.2025).
- [154] HardwareBee. *The Ultimate Guide to FPGA Architecture*. 2024. URL: <https://hardwarebee.com/the-ultimate-guide-to-fpga-architecture/> (term. wiz. 05.05.2025).
- [155] Infineon Technologies AG. *EZ-USB FX3 USB 5 Gbps Peripheral Controller*. 2025. URL: <https://www.infineon.com/cms/en/product/universal-serial-bus/usb-3.2-peripheral-controllers/ez-usb-fx3-usb-5gbps-peripheral-controller/> (term. wiz. 02.05.2025).
- [156] Future Technology Devices International Limited. *F600/FT601 Series – SuperSpeed USB3.0 ICs*. 2025. URL: <https://ftdichip.com/products/ft601q-b/> (term. wiz. 02.05.2025).
- [157] Ettus Research. *USRP*. 2025. URL: <https://www.ettus.com/> (term. wiz. 02.05.2025).
- [158] Tektronix. *Understanding FFT Overlap Processing Fundamentals*. 2021. URL: https://download.tek.com/document/37W_18839_1.pdf (term. wiz. 05.05.2025).
- [159] Weiqiang Liu, Fabrizio Lombardi i Michael Shulte. „A Retrospective and Prospective View of Approximate Computing [Point of View]”. W: *Proceedings of the IEEE* 108.3 (2020), s. 394–399.
- [160] Chih-Feng Wu i Muh-Tian Shiue. „Cost-Efficient Approximation for Magnitude of a Complex Signal”. W: *Electronics* 13.13 (2024), s. 1–11.
- [161] M. Allie i R. Lyons. „A root of less evil [digital signal processing]”. W: *IEEE Signal Processing Magazine* 22.2 (2005), s. 93–96.
- [162] R. Smyk i M. Czyżak. „Implementation of magnitude calculation of complex numbers using improved alpha max plus beta min algorithm”. W: *Zeszyty Naukowe Wydziału Elektrotechniki i Automatyki Politechniki Gdańskiej* 51 (2016), s. 173–179.
- [163] Hongxi Dong, Manzhen Wang, Yuanyong Luo, Muhan Zheng, Mengyu An, Yajun Ha i Hongbing Pan. „PLAC: Piecewise Linear Approximation Computation for All Nonlinear Unary Functions”. W: *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* 28.9 (2020), s. 2014–2027.

- [164] Minh-Hong Nguyen. „An efficient hardware logarithm generator with modified quasi-symmetrical approach for digital signal processing”. W: *International Journal of Electrical and Computer Engineering (IJECE)* 10.10 (2020), s. 4671.
- [165] Ngozi Bello i K.O. Ogbeide. „Designing a Real-time Swept Spectrum Analyser with USRP B210”. W: *Nigerian Journal of Environmental Sciences and Technology* 5.10 (2021), s. 329–339.
- [166] Michael Ossmann i Dominic Spill. *What’s on the Wireless? Automating RF Signal Identification*. 2017. URL: <https://www.blackhat.com/docs/us-17/wednesday/us-17-Ossmann-Whats-On-The-Wireless-Automating-RF-Signal-Identification-wp.pdf> (term. wiz. 19.05.2025).
- [167] Great Scott Gadgets. *Welcome to HackRF’s documentation*. 2021. URL: <https://hackrf.readthedocs.io/en/latest/> (term. wiz. 31.05.2025).
- [168] RFMD. *The RFFC5071A in ISM Band Shift Applications*. 2014. URL: <https://www.qorvo.com/products/d/da000738> (term. wiz. 31.05.2025).
- [169] MHD Saria Allahham, Mohammad F. Al-Sa’d, Abdulla Al-Ali, Amr Mohamed, Tamer Khattab i Aiman Erbad. „DroneRF dataset: A dataset of drones for RF-based detection, classification and identification”. W: *Data in Brief* 26 (2019), s. 104313.
- [170] Carolyn J. Swinney i John C. Woods. „RF Detection and Classification of Unmanned Aerial Vehicles in Environments with Wireless Interference”. W: *2021 International Conference on Unmanned Aircraft Systems (ICUAS)*. 2021, s. 1494–1498.
- [171] Boban Sazdic-Jotic, Ivan Pokrajac, Jovan Bajcetic i Boban Bondzulic. *VTI DroneSET*. 2020. URL: <https://data.mendeley.com/datasets/s6tggnp5n2/3> (term. wiz. 14.06.2025).
- [172] Sanjoy Basak, Sreeraj Rajendran, Sofie Pollin i Bart Scheers. „Autoencoder based framework for drone RF signal classification and novelty detection”. W: *2023 25th International Conference on Advanced Communication Technology (ICACT)*. 2023, s. 218–225.
- [173] Miika Vuorenmaa, Jaakko Marin, Mikko Heino, Matias Turunen i Taneli Riihonen. *Radio-Frequency Control and Video Signal Recordings of Drones*. 2020. URL: <https://doi.org/10.5281/zenodo.4264467> (term. wiz. 14.06.2025).
- [174] A.J. Onumanyi, A.M. Abu-Mahfouz i G.P. Hancke. „A comparative analysis of local and global adaptive threshold estimation techniques for energy detection in cognitive radio”. W: *Physical Communication* 29 (2018), s. 1–11.

- [175] Maxwell Oligbi, Zubair Suleiman i Caroline Alenoghena. „Advances in Adaptive Threshold Techniques in Cognitive Radio: A Survey”. W: *Journal of Innovations in Engineering and Technology Research* 2.2 (2023), s. 1–23.
- [176] Dinesh Datla, Alexander Wyglinski i Gary Minden. „A Spectrum Surveying Framework for Dynamic Spectrum Access Networks”. W: *Vehicular Technology, IEEE Transactions on* 58.11 (2009), s. 4158–4168.
- [177] Janne J. Lehtomaki, Johanna Vartiainen, Markku Juntti i Harri Saarnisaari. „Spectrum Sensing with Forward Methods”. W: *MILCOM 2006 - 2006 IEEE Military Communications conference*. 2006, s. 1–7.
- [178] Adeiza Onumanyi, Liz Onwuka, Abiodun Aibinu, Okechukwu Ugweje i Momoh Salami. „A Modified Otsu’s Algorithm for Improving the Performance of the Energy Detector in Cognitive Radio”. W: *AEU - International Journal of Electronics and Communications* 79.05 (2017), s. 53–63.
- [179] G. Bradski. *The OpenCV Library*. 2025. URL: <https://opencv.org> (term. wiz. 22.06.2025).
- [180] Dae-Il Noh, Seon-Geun Jeong, Huu-Trung Hoang, Quoc-Viet Pham, Thien Huynh-The, Mikio Hasegawa, Hiroo Sekiya, Sun-Young Kwon, Sang-Hwa Chung i Won-Joo Hwang. „Signal Preprocessing Technique With Noise-Tolerant for RF-Based UAV Signal Classification”. W: *IEEE Access* 10 (2022), s. 134785–134798.
- [181] Olusiji .O. Medaiyese, Martins Ezuma, Adrian P. Lauf i Ismail Guvenc. „Wavelet transform analytics for RF-based UAV detection and identification system using machine learning”. W: *Pervasive and Mobile Computing* 82 (2022), s. 101569.
- [182] Tomasz Gandor. *Detekcja obiektów w obrazach cyfrowych z użyciem uczenia głębokiego w warunkach stratnej kompresji obrazu*. 2022. URL: https://pja.edu.pl/wp-content/uploads/2023/03/Tomasz_Gandor_rozprawa.pdf (term. wiz. 20.05.2025).
- [183] Joseph Redmon, Santosh Divvala, Ross Girshick i Ali Farhadi. „You Only Look Once: Unified, Real-Time Object Detection”. W: *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. 2016, s. 779–788.
- [184] Sanjoy Basak, Sreeraj Rajendran, Sofie Pollin i Bart Scheers. „Combined RF-Based Drone Detection and Classification”. W: *IEEE Transactions on Cognitive Communications and Networking* 8.1 (2022), s. 111–120.
- [185] T.Quach Anna i Randall D. Reese. „YOLO for Radio Frequency Signal Classification”. W: *2024 IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN)*. 2024, s. 177–178.

- [186] Tijeni Delleji i Feten Slimeni. „RF-YOLO: a modified YOLO model for UAV detection and classification using RF spectrogram images”. W: *Telecommunication Systems* 88.02 (2025), s. 1–16.
- [187] Nidhal Jegham, Chan Young Koh, Marwan Abdelatti i Abdeltawab Hendawi. *YOLO Evolution: A Comprehensive Benchmark and Architectural Review of YOLOv12, YOLOv11, and Their Previous Versions*. 2025. URL: <https://arxiv.org/abs/2411.00201> (term. wiz. 12.07.2025).
- [188] Jiang Tianyou i Zhong Yang. *ODverse33: Is the New YOLO Version Always Better? A Multi Domain benchmark from YOLO v5 to v11*. 2025. URL: <https://arxiv.org/abs/2502.14314> (term. wiz. 12.07.2025).
- [189] Haidy Elghamrawy, Malek Karaim, Mohamed Tamazin i Aboelmaged Noureldin. „Experimental Evaluation of the Impact of Different Types of Jamming Signals on Commercial GNSS Receivers”. W: *Applied Sciences* 10.12 (2020), s. 1–15.
- [190] Mengyu Ding, Wu Chen i Weihao Ding. „Performance Analysis of a Normal GNSS Receiver Model under Different Types of Jamming Signals”. W: *Measurement* 214 (mar. 2023), s. 1–13.
- [191] Jansen Pim. *The impact of jamming and spoofing on GNSS signals*. 2022. URL: <https://repository.tudelft.nl/record/uuid:4085302c-ae13-4615-b437-3d7dad64ed44> (term. wiz. 02.08.2025).
- [192] Olcay Yiğit, Havva Bilişik Bakbak, Eren Demir, Radosveta Sokullu i Korkut Yegin. „GPS Signal Channel Modeling and Verification”. W: *Procedia Computer Science* 113.09 (2017), s. 621–626.
- [193] Daniele Borio, Fabio Dovis, Heidi Kuusniemi i Letizia Lo Presti. „Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers”. W: *Proceedings of the IEEE* 104.6 (2016), s. 1233–1245.
- [194] Syed Ali Kazim. *Enhancing Jamming Resilience in GNSS-based Localization for Safety-Critical Land Transportation : Towards an Optimized Mitigation Approach Focusing User-Requirements*. 2024. URL: <https://theses.hal.science/tel-04952405v1> (term. wiz. 09.08.2025).
- [195] Ali Reda, Tamer Mekkawy, Theodoros A. Tsiftsis i Ashraf Mahran. „Deep Learning Approach for GNSS Jamming Detection-Based PCA and Bayesian Optimization Feature Selection Algorithm”. W: *IEEE Transactions on Aerospace and Electronic Systems* 60.6 (2024), s. 8349–8363.
- [196] Xiangjun Li, Lei Chen, Zukun Lu, Feixue Wang, Wenxiang Liu, Wei Xiao i Peiguo Liu. „Overview of Jamming Technology for Satellite Navigation”. W: *Machines* 11.7 (2023), s. 1–29.

-
- [197] uBlox. *EVK-F9P, u-blox F9P high precision GNSS evaluation kit*. 2025. URL: <https://www.u-blox.com/en/product/evk-f9p> (term. wiz. 09.08.2025).
- [198] Kentaro Nishimori, Koshiro Kitao i Tetsuro Imai. „Interference-Based Decode and Forward Scheme Using Relay Nodes in Heterogeneous Networks”. W: *International Journal of Antennas and Propagation* 2012.10 (2012), s. 1–10.
- [199] Mehmet Akif Durmaz, Hakan Alakoca, Günes Karabulut Kurt i Cem Ayyıldız. „Chirp subcarrier jamming attacks: an OFDM based smart jammer design”. W: *2017 16th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*. 2017, s. 1–5.
- [200] Grecia Romero, Virginie Deniau i Eric Pierre Simon. „Mitigation Technique to Reduce the Wi-Fi Susceptibility to Jamming Signals”. W: *2018 2nd URSI Atlantic Radio Science Meeting (AT-RASC)*. 2018, s. 1–3.
- [201] T. Charles Clancy. „Efficient OFDM Denial: Pilot Jamming and Pilot Nulling”. W: *2011 IEEE International Conference on Communications (ICC)*. 2011, s. 1–5.
- [202] Hanif Rahbari, Marwan Krunz i Loukas Lazos. „Swift Jamming Attack on Frequency Offset Estimation: The Achilles’ Heel of OFDM Systems”. W: *IEEE Transactions on Mobile Computing* 15.5 (2016), s. 1264–1278.
- [203] Li Li, Shulin Tian, Jianguo Huang i Peng Zhang. „Efficient and unrecognizable OFDM jamming by failing the cyclic prefix functionality”. W: *2017 9th International Conference on Wireless Communications and Signal Processing (WCSP)*. 2017, s. 1–6.