Przegląd 4/2024
TELEKOMUNIKACYJNY
WIADOMOŚCI TELEKOMUNIKACYJNE

Dwumiesięcznik Stowarzyszenia Elektryków Polskich

ISSN 1230-3496, e-ISSN 2449-7487
**Cena: 60 zł (w tym 8% VAT)**

WYDAWNICTWO *SIGMA-NOT*

# Konferencja Radiokomunikacji i Teleinformatyki

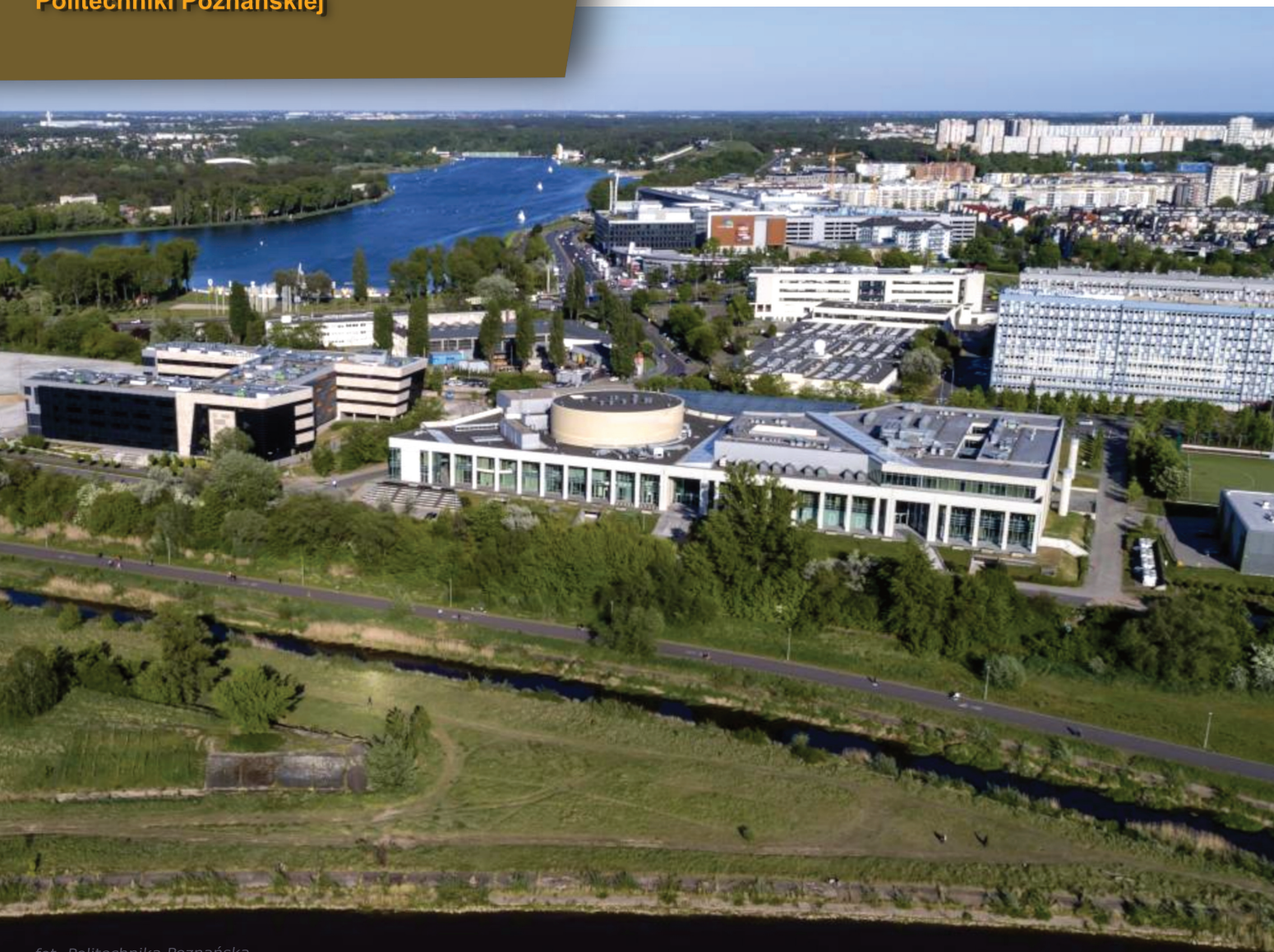
## Poznań 11-13 września 2024

**Centrum Wykładowo-Konferencyjne Politechniki Poznańskiej**

KRiT 2024

00110010 00110000 00110010 00110100

01001011 01010010 01101001 01010100



**Szanowni Państwo!**

Oddajemy Państwu do rąk specjalny numer zasłużonego czasopisma Przegląd Telekomunikacyjny. Numer ten poświęcony jest Konferencji Radiokomunikacji i Teleinformatyki, która odbywa się w Centrum Wykładowo-Konferencyjnym Politechniki Poznańskiej w dniach 11–13 września 2024 r. W tym roku konferencja jest organizowana przez Instytut Radiokomunikacji oraz Instytut Sieci Teleinformatycznych Politechniki Poznańskiej.

W ostatnich latach obserwujemy niezwykle dynamiczny postęp zarówno w dziedzinie radiokomunikacji, jak i teleinformatyki. Dziedziny te przenikają się coraz bardziej. Przykładem tego procesu jest rozwój standardów radiokomunikacji piątej i szóstej generacji, w której obok coraz doskonalszych technologii warstwy fizycznej i ich ekspansji w kierunku coraz wyższych zakresów częstotliwości, niezwykle dynamicznie rozwijają się techniki sieciowe i informatyczne mające na celu zarządzanie przepływem coraz bardziej zróżnicowanych rodzajów informacji, ich przechowywaniem i ochroną przed nieuprawnionym dostępem oraz wykorzystaniem. Warta podkreślenia jest również ewolucja treści i charakteru ruchu telekomunikacyjnego wynikająca m.in. z rosnącego udziału treści multimedialnych oraz z dynamicznego rozwoju usług o charakterze chmurowym. Lektura przedstawionych w tym numerze Przeglądu Telekomunikacyjnego referatów uzmysławia nam, że w coraz szerszym zakresie rozwiązania radiokomunikacyjne, multimedialne i teleinformatyczne stosują techniki uczenia maszynowego i sztucznej inteligencji, które stały się znaczącym tematem tegorocznej konferencji. Zjawisko to jest widoczne również w zagadnieniach dotyczących cyberbezpieczeństwa, co także znalazło swój wyraz w tematyce naszej konferencji.

Niniejszy numer specjalny zawiera w wersji tradycyjnej sześć referatów plenarnych, 81 referatów w wersji elektronicznej nadesłanych do organizatorów konferencji i poddanych recenzjom a także sześć referatów przygotowanych przez laureatów konkursu Fundacji Wspierania Rozwoju Radiokomunikacji i Technik Multimedialnych działającej przy Politechnice Warszawskiej. Oprócz sesji plenarnych i technicznych oferujemy Państwu panel poświęcony rozwojowi technik satelitarnych w Polsce a także sesje firmowe.

W tym miejscu pragniemy podziękować firmom szczodrze wspierającym naszą konferencję: firmie Systemics PAB (Sponsor Rubinowy), Tieto Poland Sp. z o.o. (Sponsor Srebrny) oraz Naukowej i Akademickiej Sieci Komputerowej – Państwowemu Instytutowi Badawczemu a także Rimedo Labs (Sponsorzy). Bardzo wysoko cenimy także niezawodny udział firmy Sprint S.A. w konferencji jako fundatora statuetki Złotego Cyborga wręczanej co roku kilku wybitnym przedstawicielom świata nauki i biznesu z zakresu szeroko rozumianej telekomunikacji, teleinformatyki i multimediów.

Wszystkim autorom referatów i uczestnikom konferencji życzymy wielu sukcesów naukowych, ustanowienia owocnych kontaktów zawodowych i niezapomnianych wrażeń z pobytu w murach Politechniki Poznańskiej.

W imieniu Komitetu Programowego KRiT 2024

**Prof. dr hab. inż. Krzysztof Wesołowski**
**Współprzewodniczący Komitetu Programowego**

**Dr hab. inż. Piotr Zwierzykowski, prof. uczelni, Współprzewodniczący Komitetu Programowego**

4/2024

DWUMIESIĘCZNIK STOWARZYSZENIA
ELEKTRYKÓW POLSKICH
WYDAWANY PRZY WSPÓŁPRACY
KOMITETU
ELEKTRONIKI I TELEKOMUNIKACJI
POLSKIEJ AKADEMII NAUK

# Przegląd TELEKOMUNIKACYJNY

TELE–RADIO–ELEKTRONIKA–INFORMATYKA

ROK ZAŁOŻENIA 1928 • ROCZNIK XCVIII • ISSN 1230-3496



**Adres redakcji:**
ul. Czackiego 3/5, 00-043 Warszawa
**www.przegladtelekomunikacyjny.pl**
**przeg.tel@sigma-not.pl**

**Skład:**
Studio DTP Wydawnictwa SIGMA-NOT,
Katarzyna Paszkowska

**Zamówienia na reklamę** przyjmuje Redakcja
lub Dział Reklamy i Marketingu,
ul. Ratuszowa 11, 03-450 Warszawa
tel. 22 827 43 65, e-mail: **reklama@sigma-not.pl**

**Zakład Poligrafii i Kolportażu**
**Wydawnictwa SIGMA-NOT**
ul. ks. J. Popiełuszki 19/21, 01-595 Warszawa,
tel. 22 840 35 89; tel. 22 840 59 49, 22 891 13 74,
e-mail: **prenumerata@sigma-not.pl**



**Indeks 35722 Nakład do 500 egz** (w tym wersja elektroniczna)

WYDAWNICTWO SIGMA-NOT

03-450 Warszawa, ul. Ratuszowa 11
tel.: 22 818-09-18, 22 818-98-32
www.sigma-not.pl
sekretariat@sigma-not.pl

## SPIS TREŚCI • CONTENTS

CYBERBEZPIECZEŃSTWO: JASNE I CIEMNE STRONY WSPÓŁCZESNYCH TECHNOLOGII
CYBERSECURITY: THE BRIGHT AND DARK SIDES OF TODAY'S TECHNOLOGIE
*G. BOROWIK, A. FELKNER, A. KOZAKIEWICZ* ..... 7

ZASTOSOWANIE METOD UCZENIA MASZYNOWEGO W SIECIACH TELEINFORMATYCZNYCH
APPLICATION OF MACHINE LEARNING METHODS N COMMUNICATION NETWORKS
*K. WALKOWIAK, A. KNAPIŃSKA, P. LECHOWICZ* ..... 18

FALE MILIMETROWE I TERAHERCOWE W SYSTEMACH KOMÓRKOWYCH: WYKORZYSTANIE, MODELOWANIE PROPAGACJI I WPŁYW NA ARCHITEKTURĘ SIECI
MILLIMETER AND TERAHERTZ WAVES IN CELLULAR SYSTEMS: UTILIZATION, PROPAGATION MODELING AND IMPACT ON NETWORK ARCHITECTURE
*S. HAUSMAN* ..... 25

KRAJOWE LABORATORIUM SIECI I USŁUG PL 5G: KIERUNKI BADAŃ I PERSPEKTYWY ROZWOJU TECHNIKI 5G/6G
5G NATIONAL LABORATORY: PERSPECTIVE AND RESEARCH DIRECTIONS
*A. BĘBEN, M. SOSNOWSKI, W. JÓŹWIAK, J. WOŹNIAK, K. GIERŁOWSKI, M. HOEFT, M. NATKANIEC, P. BORYŁO, B. BELTER, M. FURMANN, P. SCHAUER, Ł. FALAS, A. WARZYŃSKI, I. MICHALSKI, D. WIĘCEK* ..... 33

RECENT ADVANCES IN OPEN RAN SYSTEMS
AKTUALNY STAN STANDARYZACJI SYSTEMÓW OTWARTYCH SIECI DOSTĘPOWYCH (OPEN RAN)
*M. DRYJAŃSKI* ..... 43

EFEKTYWNE ENERGETYCZNIE WIELODOSTĘPOWE PRZETWARZANIE BRZEGOWE W SIECI 5G
ENERGY EFFICIENT MULTI-ACCESS EDGE COMPUTING IN 5G NETWORK
*P. KRYSZKIEWICZ* ..... 50


Dwumiesięcznik **Przegląd Telekomunikacyjny i Wiadomości Telekomunikacyjne** znajduje się w wykazie czasopism naukowych Ministerstwa Nauki i Szkolnictwa Wyższego.

Niniejszy zeszyt (4/2024) naszego dwumiesięcznika jest związany z KONFERENCJĄ RADIOKOMUNIKACJI i TELEINFORMATYKI 2024. Konferencja powstała w wyniku połączenia Krajowej Konferencji Radiokomunikacji, Radiofonii i Telewizji (KKRRiT) oraz Krajowego Sympozjum Telekomunikacji i Teleinformatyki (KSTiT). Organizatorem tegorocznej KRiT jest Instytut Radiokomunikacji oraz Instytut Sieci Teleinformatycznych Politechniki Poznańskiej.

**Zeszyt zawiera całość materiałów konferencyjnych. Referaty plenarne są drukowane, a pełne teksty wszystkich referatów są zamieszczone na Portalu Informacji Technicznej SIGMA-NOT z nieodpłatnym dostępem: https://sigma-not.pl/zeszyt-7541-przeglad-telekomunikacyjny-2024-4.html.**

Stanowią one integralną część zeszytu. Wszystkie artykuły i referaty są recenzowane. Podstawowe informacje na temat konferencji znajdą Państwo w artykule wstępnym (II str. okładki), przygotowanym przez: prof. dr hab. inż. Krzysztofa Wesołowskiego oraz dr hab. inż. Piotra Zwierzykowskiego – profesora uczelni, współprzewodniczących Komitetu Programowego KRiT 2024: .

# LISTA RECENZENTÓW

Marek Amanowicz, Sławomir Ambroziak, Andrzej Bęben, Piotr Chołda, Marek Domański, Janusz Dudczyk, Róża Goścień, Maciej Grzybkowski, Sławomir Hanczewski, Sławomir Hausman, Łukasz Januszkiewicz, Wojciech Kabaciński, Sylwester Kaczmarek, Jan Kelner, Adrian Kliks, Mirosław Klinkowski, Katarzyna Kosek-Szott, Maciej Krasicki, Rafał Krenz, Paweł Kryszkiewicz, Mikołaj Leszczuk, Jarosław Michalak, Józef Modelski, Jordi Mongay Batalla, Marek Natkaniec, Marcin Niemiec, Andrzej Pach, Grzegorz Pastuszak, Zbigniew Piotrowski, Remigiusz Rajewski, Piotr Remlein, Jarosław Sadowski, Wiktor Sęga, Kajetana Snopek, Maciej Stasiak, Jacek Stefański, Marek Suchański, Wojciech Sułek, Szymon Szott, Halina Tarasiuk, Krzysztof Walkowiak, Krzysztof Wesołowski, Robert Wójcik, Yevhen Yashchyshyn, Zbigniew Zakrzewski, Ryszard Zieliński, Mariusz Żal.

# Referaty sesji tematycznych zamieszczone na Portalu Informacji Technicznej SIGMA-NOT

## ST01. SZTUCZNA INTELIGENCJA W SYSTEMACH RADIOWYCH – I


**S. ZARĘBSKI, P. CHOŁDA, K. RUSEK**
ENHANCING SOFTWARE TESTING OF 5G BASE STATIONS WITH LLM-DRIVEN ANALYSIS . . . . . 57

**K. SZCZĘCH, S. SZOTT**
KONCEPCJA INTERFEJSU RADIOWEGO OPARTEGO NA UCZENIU MASZYNOWYM W PROJEKCIE MLDR . . . . . 61

**T. WALCZYNA, Z. PIOTROWSKI**
METODA PREDYKCJI ZAJĘTOŚCI PASMA W KANALE RADIOWYM W OPARCIU O GŁĘBOKIE SIECI NEURONOWE. . . . . 65

**Ł. KUŁACZ, A. KLIKS**
ROZPROSZONE WYKRYWANIE ZAJĘTOŚCI WIDMA OPARTE NA UCZENIU FEDERACYJNYM . . . . . 69


## ST02. BEZPIECZEŃSTWO SIECI I SYSTEMÓW TELEINFORMATYCZNYCH


**P. POPIOŁEK, J. BIENIASZ**
PRAKTYCZNA REALIZACJA ATAKÓW OMIJANIA SYSTEMÓW WYKRYWANIA WŁAMAŃ W SIECIACH . . . . . 73

**F. RAKOWSKI, P. OSTAPOWICZ, M. STRÓŻYK, M. GŁOWIAK, M. SMOLIK**
ROZWÓJ I ZASTOSOWANIE SYSTEMU MONITORINGU URZĄDZEŃ AUTOMATYKI PRZEMYSŁOWEJ SMUAP . . . . . 77

**M. STYPIŃSKI**
WPŁYW PARAMETRÓW SIECI TYPU TREE PARITY MACHINE NA BEZPIECZEŃSTWO ALGORYTMU WYRÓWNUJĄCEGO WAGI. . . . . 81

**S. HANCZEWSKI, P. REMLEIN**
WYBRANE METODY WYKRYWANIA I PRZECIWDZIAŁANIA ATAKOM NA INFRASTRUKTURĘ DOSTĘPOWĄ I APLIKACJE SIECI 5G . . . . . 85


## ST03. SYSTEMY RADIONAWIGACYJNE IRADIOLOKALIZACYJNE – I


**J. SADOWSKI, J. STEFAŃSKI**
ESTYMACJA POŁOŻENIA I ORIENTACJI W SYSTEMIE LOKALIZACYJNYM Z CZĘŚCIOWĄ SYNCHRONIZACJĄ WĘZŁÓW REFERENCYJNYCH . . . . . 89

**K. BEDNARZ, J. WOJTUŃ, C. ZIÓŁKOWSKI**
OGRANICZENIA WIDMOWEJ METODY ESTYMACJI CZĘSTOTLIWOŚCI W SENSORZE LOKALIZACYJNYM ZBUDOWANYM NA KOMPUTERZE JEDNOPŁYTKOWYM. . . . . 93

**M. KOŁAKOWSKI**
SELEKCJA WĘZŁÓW POPRZEZ MINIMALIZACJĘ BŁĘDU LOKALIZACJI W WĄSKICH PRZEJŚCIACH. . . . . 97

**P. OLEKSY**
RADIOLOKACJA ENDOSKOPÓW KAPSUŁKOWYCH WYKORZYSTUJĄCA ADAPTACYJNY ALGORYTM OPARTY NA DETEKCJI FAZY . . . . . 101


## ST04. ASPEKTY SIECI RDZENIOWYCH 5G I 6G – I


**M. KLINKOWSKI**
ANALIZA KOSZTOWA PASYWNEJ OPTYCZNEJ SIECI XHAUL Z AGREGACJĄ RUCHU W WARSTWIE OPTYCZNEJ . . . . . 105

**K. KOSMOWSKI, R. BRYŚ, A. DUDKO**
ATAKI NA PROTOKÓŁ PFCP SIECI SZKIELETOWEJ 5G ORAZ METODY ICH IDENTYFIKACJI . . . . . 109

**K. SADURA**
METODA SKALOWANIA WYDAJNOŚCI FUNKCJI UPF W SIECIACH 5G BAZUJĄCA NA SI . . . . . 113

**W. JÓŹWIAK**
ORKIESTRACJA APLIKACJI I FUNKCJI UPF W SIECIACH B5G . . . . . 117

## ST05. SZTUCZNA INTELIGENCJA W SYSTEMACH RADIOWYCH – II

**Ł. RYBAK, J. DUDCZYK, P. MAZUR**
ALGORYTMY SZTUCZNEJ INTELIGENCJI W PRZETWARZANIU DANYCH ROZPOZNANIA RADIOELEKTRONICZNEGO ELINT . . . . . 121

**A. OLEJNICZAK, J. SADOWSKI**
GŁĘBOKIE UCZENIE DO KOREKCJI FAZY SYGNAŁÓW GMSK W RZECZYWISTYM ŚRODOWISKU WEWNĄTRZBUDYNKOWYM . . . . . 125

**W. FLAKOWSKI, M. KRASICKI, R. KRENZ**
METODY DETEKCJI ORAZ ROZPOZNAWANIA SYGNAŁÓW DRONÓW . . . . . 129

**I. ZAINUTDINOV, R. KRENZ**
OPTYMALIZACJA PRZEPUSTOWOŚCI ŁĄCZA SATELITARNEGO ZA POMOCĄ UCZENIA MASZYNOWEGO . . . . . 135

## ST06. KRYPTOGRAFIA I MECHANIZMY CYBERBEZPIECZEŃSTWA

**M. BOROWSKI, M. BUCZKOWSKI**
KRYPTOGRAFICZNA OCHRONA UŻYTKOWNIKÓW SIECI 5G PRZED ATAKIEM TYPU MITM PRZY UŻYCIU WĘZŁÓW PRZEKAŹNIKOWYCH . . . . . 139

**M. BOROWSKI, M. BUCZKOWSKI**
POTRZEBA STAŁEGO KRYPTOGRAFICZNEGO ZABEZPIECZENIA INTEGRALNOŚCI DANYCH PŁASZCZYZNY UŻYTKOWNIKA SIECI 5G . . . . . 143

**M. BAJOR, P. CHOŁDA, B. GDOWSKI, D. KARCZ, M. NIEMIEC, F. OPIŁKA, M. STYPIŃSKI, W. SZCZEPANIK**
WYZWANIA I PERSPEKTYWY WDROŻENIA EFEKTYWNEJ KRYPTOGRAFII POSTKWANTOWEJ . . . . . 147

## ST07. SYSTEMY RADIONAWIGACYJNE I RADIOLOKALIZACYJNE – II

**M. KOŁAKOWSKI**
METODA LOKALIZACJI UWZGLĘDNIAJĄCA CHARAKTERYSTYCZNE TRAJEKTORIE RUCHU . . . . . 151

**J. SADOWSKI, O. BŁASZKIEWICZ, K. CWALINA, A. OLEJNICZAK, P. RAJCHOWSKI, J. STEFAŃSKI**
POMIAROWA WERYFIKACJA EFEKTYWNOŚCI PRACY ASYNCHRONICZNEJ METODY JEDNOCZESNEJ ESTYMACJI POŁOŻENIA I ORIENTACJI OBIEKTU . . . . . 155

**V. DJAJA-JOŚKO, J. TUCHOWSKI**
SYSTEM DO LOKALIZOWANIA OSÓB W POMIESZCZENIACH Z WYKORZYSTANIEM CZUJNIKÓW PODCZERWIENI . . . . . 159

**K. BŁASZCZUK, Z. PIOTROWSKI**
PRZEGLĄD METOD NAMIERZANIA EMITERÓW RADIOWYCH . . . . . 163

## ST08. ASPEKTY SIECIOWE INTERNETU RZECZY

**A. RUIZ ALVAREZ, A. VEJAR, F. MARZUK**
LEVERAGING LORAWAN FOR INTELLIGENT GARBAGE COLLECTION IN CITIES USING MATERIAL COMPOSITION DATA FROM SMART BINS . . . . . 167

**J. SZEWCZYK, P. REMLEIN, M. NOWAK, W. CIEŚLAK**
WPŁYW METOD AKTYWACJI URZĄDZEŃ PRACUJĄCYCH W SIECI LORA WAN NA BEZPIECZEŃSTWO SYSTEMU . . . . . 171

**D. WANAT, D. JUSZKA, M. LESZCZUK, L. JANOWSKI**
MANIANA: URZĄDZENIE IOT DO TESTOWANIA QOS I QOE APLIKACJI W SIECI DOMOWEJ . . . . . 175

**A. FRANKIEWICZ, K. GROCHLA**
OCENA WYDAJNOŚCI MECHANIZMU RETRANSMISJI TS011_1.0.0 W SIECIACH LORAWAN . . . . . 179

## ST09. ZASTOSOWANIE METOD SZTUCZNEJ INTELIGENCJI W PRZETWARZANIU DANYCH MULTIMEDIALNYCH

**MIELOCH, D. KLÓSKA, A. DZIEMBOWSKI, B. SZYDEŁKO, A. GRZELKA, J. STANKOWSKI**
TWORZENIE WIELOWIDOKOWYCH SEKWENCJI DLA WIZJI WSZECHOGARNIAJĄCEJ . . . . . 183

**MEHRUNNISA, D. JUSZKA, Y. ZHANG, M. LESZCZUK**
COMPARATIVE PERFORMANCE ANALYSIS OF DEEP LEARNING ARCHITECTURES IN UNDERWATER IMAGE CLASSIFICATION . . . . 187

**M. BISTROŃ, Z. PIOTROWSKI**
INTELIGENTNY WATERMARKING WIDEO: WYZWANIA TECHNICZNE I PERSPEKTYWY ROZWOJU Z WYKORZYSTANIEM SZTUCZNEJ INTELIGENCJI . . . . . 191

**P. DUSZEJKO, Z. PIOTROWSKI**
ZASTOSOWANIE ATENCJI W SIECIACH NEURONOWYCH DO ZAAWANSOWANEGO ZNAKOWANIA WODNEGO OBRAZÓW W WYSOKIEJ ROZDZIELCZOŚCI: ANALIZA EFEKTYWNOŚCI I METRYK . . . . . 195

**D. KOSZEWSKI**
SYSTEM AUTOMATYCZNEGO MIKSOWANIA SYGNAŁÓW MUZYCZNYCH Z WYKORZYSTANIEM JEDNOWYMIAROWYCH AUTOENKODERÓW WAVE-U-NET . . . . . 199

## ST10. ASPEKTY RADIOWE SIECI 5G I 6G – I

**J. MAGIERA, P. RAJCHOWSKI**
CELOWE ZANIECZYSZCZANIE PILOTÓW W ŁĄCZU W GÓRĘ W INTERFEJSIE 5G NR . . . . . 203

**M. HOFFMANN**
FORMOWANIE KLASTRÓW OBSŁUGUJĄCYCH W SIECI 6G OPEN RAN O ARCHITEKTURZE ZORIENTOWANEJ NA UŻYTKOWNIKA . . . . . 208

**P. RAJCHOWSKI, L. M. CORREIA, K. K. CWALINA**
MODELOWANIE DOKŁADNOŚCI RADIOLOKALIZOWANIA W RÓŻNYCH WARUNKACH ŚRODOWISKOWYCH PRZY WYKORZYSTANIU INTERFEJSU RADIOWEGO 5G-NR . . . . . 213

**K. WESOŁOWSKI**
METODA WYDZIELANIA SYGNAŁU INTENCJONALNYCH ZAKŁÓCEŃ W TRANSMISJI RADIOWEJ MIMO . . . . . 217

## ST11. BEZPRZEWODOWE SIECI LOKALNE, SENSOROWE I AD-HOC

**Z. ŁASKARZEWSKI, K. GROCHLA**
EFEKTYWNOŚĆ SCHEMATU KOMUNIKACJI LICZNIKÓW MEDIÓW W PROCESIE ZDALNEGO ODCZYTU OBCHODZONEGO . . . . . 221

**A. KUBOWICZ, J. ŁOPATKA**
KONCEPCJA KOGNITYWNEJ TRANSMISJI WYKORZYSTUJĄCEJ ROZPRASZANIE WIDMOWE ZA POMOCĄ ULTRA SZYBKIEGO SKAKANIA PO CZĘSTOTLIWOŚCIACH . . . . . 225

**T. JÓŹWIK**
MODEL OPTYMALIZACJI DLA ENERGOOSZCZĘDNEGO ROUTINGU UNICAST W SIECIACH FANET . . . . . 229

**Z. ZAKRZEWSKI**
ZASTOSOWANIE INTERFEJSÓW D-ROF/A-ROF W SIECIACH 802.11 NASTĘPNYCH GENERACJI . . . . . 233

## ST12. JAKOŚĆ USŁUG I NIEZAWODNOŚĆ SIECI TELEINFORMATYCZNYCH

**P. JURKIEWICZ, M. RZEPKA, P. JAGLARZ, J. DOMŻAŁ, R. WÓJCIK**
IMPLEMENTACJA RUTERA Z MECHANIZMEM ADAPTACYJNEGO MULTI-HOMINGU . . . . . 237

**K. MAŚLANKA, J. WOJTUŃ, J. M. KELNER**
OCENA PARAMETRÓW $Q_0S$ USŁUGI TRANSMISJI DANYCH Z WYKORZYSTANIEM MODUŁÓW DTC SOL8SDR DLA ROZWIĄZAŃ DRONOWYCH . . . . . 241

**S. UDDIN, W. UR RAHMAN, M. GREGA, M. LESZCZUK**
QOE BASED OBJECTIVE ANALYSIS OF LOW-LATENCY ALGORITHMS IN DASH.JS . . . . . 245

**P. ANDRULONIW, P. ZWIERZYKOWSKI, K. KOWALIK**
SUBIEKTYWNE POSTRZEGANIE POJEDYNCZYCH ZNIEKSZTAŁCEŃ W TELEWIZJI OPARTEJ O STRUMIENIOWANIE ADAPTACYJNE . . . 249

**S. KACZMAREK, K. ZALEWSKI**
REALIZACJA PRÓBNIKA SYSTEMU REJESTROWANIA I MONITOROWANIA PARAMETRÓW JAKOŚCIOWYCH STOSUJĄCEGO STANDARD IPFIX . . . . . 253

## ST13. TECHNIKA ANTENOWA I MIKROFALOWA

**R. PRZESMYCKI, M. BUGAJ, B. DUDZIŃSKI, L. NOWOSIELSKI**
ANTENA MIKROPASKOWA NA PASMO HIGH-BAND SYSTEMU 5G . . . . . 260

**Ł. JANUSZKIEWICZ, I. NOWAK, K. KROPIDŁOWSKI**
ANTENA TEKSTYLNA NASOBNEGO SYSTEMU PRZESYŁANIA OBRAZU . . . . . 264

**P. HATKA, D. BRZĄKAŁA, M. GARCZYK, P. PŁACZKIEWICZ, M. SIERADZKA, C. PRENTKI, T. JAWORSKI, K. CICHOŃ, A. KLIKS**
CHARAKTERYSTYKA ODBICIOWA INTELIGENTNYCH MATRYC ANTENOWYCH . . . . . 258

**M. URBAŃSKI**
ROZWÓJ SYSTEMÓW GENERACJI I DYSTRYBUCJI SYGNAŁÓW REFERENCYJNYCH W.CZ. DLA LINIOWYCH AKCELERATORÓW CZĄSTEK ELEMENTARNYCH . . . . . 272

## ST14. ASPEKTY RADIOWE SIECI 5G I 6G – II

**Ł. JOPEK, S. GRABAREK, K. SIKORSKA**
MODELOWANIE NIESNELLOWSKICH ODBIĆ FAL RADIOWYCH OD METAPOWIERZCHNI . . . . . 276

**A. SAMORZEWSKI, A. KLIKS**
PROPAGACJA SYGNAŁU RADIOWEGO W SYSTEMACH 5G WYPOSAŻONYCH W MATRYCE IPR . . . . . 280

**M. SIERADZKA, C. PRENTKI, T. JAWORSKI, P. HATKA, DAWID BRZĄKAŁA, MARCEL GARCZYK, PAWEŁ PŁACZKIEWICZ, Ł. KUŁACZ, P. KRYSZKIEWICZ, A. KLIKS**
UŻYCIE OGRANICZONEJ KSIĄŻKI KODOWEJ DLA KONFIGUROWALNYCH MACIERZY ANTENOWYCH . . . . . 284

**O. BŁASZKIEWICZ, J. SADOWSKI, P. RAJCHOWSKI**
ANALIZA POSTACI SYGNAŁU SYNCHRONIZACYJNEGO NPSS W NB-IOT . . . . . 288

**O. BŁASZKIEWICZ, J. MAGIERA, A. OLEJNICZAK, P. RAJCHOWSKI, J. SADOWSKI, J. STEFAŃSKI, K. K. CWALINA**
FRAMEWORK INTERFEJSU RADIOWEGO NB-IOT . . . . . 292

## ST15. PROPAGACJA FAL RADIOWYCH

**T. WALCZYNA, J. WOJTUŃ, C. ZIÓŁKOWSKI, B. ULJASZ**
ANALITYCZNY MODEL PROFILU GĘSTOŚCI ELEKTRONÓW JAKO WYNIK PRZETWARZANIA OBRAZOWEGO DANYCH POMIAROWYCH W JONOGRAMÓW . . . . . 296

**M. MOSKAL, M. KRYK, K. MALON, JAN M. KELNER**
MAPY TŁUMIENIA PROPAGACYJNEGO Z UWZGLĘDNIENIEM WARSTWY BUDYNKÓW . . . . . 300

**J. KOSTUJ, K. DALIL, M. MAĆKOWSKI-NOWAK, D. KARNAFEL, K. CICHOŃ**
POMIARY TŁUMIENIA SYGNAŁU RADIOWEGO WEWNĄTRZ SALI WYKŁADOWEJ . . . . . 304

**N. GLONTI, M. SIERADZKA, C. PRENTKI, K. CICHOŃ, J. SZÓSTKA**
PROJEKTOWANIE I WERYFIKACJA POMIAROWA LINII TEM . . . . . 308

**M. WARECKA**
ZWIĘKSZENIE EFEKTYWNOŚCI METODY ELEMENTÓW SKOŃCZONYCH Z WYKORZYSTANIEM WŁASNOŚCI GEOMETRII STRUKTUR. . . . . 312

## ST16. BADANIE JAKOŚCI TREŚCI MULTIMEDIALNYCH

**J. STANKOWSKI, B. SOJKA, T. GRAJEK, A. DZIEMBOWSKI**
SPÓJNA CZASOWO OBIEKTYWNA MIARA JAKOŚCI DLA WIZJI WSZECHOGARNIAJĄCEJ . . . . . 316

**T. KONASZYŃSKI, A. DUTTA, D. JUSZKA, M. LESZCZUK**
CZY W BADANIACH QOE POWINNO SIĘ OGRANICZAĆ DOSTĘP TESTEROM W ZŁYM STANIE PSYCHOFIZYCZNYM? . . . . . 320

**A. DUTTA, T. KONASZYNSKI, D. JUSZKA, M. LESZCZUK**
A CROWDSOURCING STUDY OF VIDEO QUALITY. . . . . 324

**J. STANKOWSKI, W. NOWAK, T. GRAJEK, A. DZIEMBOWSKI**
MIARA PODOBIEŃSTWA STRUKTURALNEGO DLA WIZJI WSZECHOGARNIAJĄCEJ . . . . . 328

**G. JEKATERYŃCZUK, Z. PIOTROWSKI**
PORÓWNANIE JAKOŚCI AUDIO WYBRANEJ METODY ZNAKOWANIA WODNEGO DLA SYGNAŁU MOWY, MUZYKI KLASYCZNEJ I POPULARNEJ . . . . . 332

## ST17. SYSTEMY I SIECI KOMÓRKOWE

**M. M. H. ALKALSH, A. KLIKS**
ADAPTACYJNE RÓWNOWAŻENIE OBCIĄŻENIA DLA PRZYSZŁYCH SIECI BEZPRZEWODOWYCH: PODEJŚCIE OKRESOWE . . . . . 331

**D. ZMYSŁOWSKI**
J. M. KELNER, IDENTYFIKACJA OPERATORA NA PODSTAWIE WSKAŹNIKÓW JAKOŚCI SYGNAŁU RADIOWEGO – ZARYS PODEJŚCIA . . . . . 340

**M. RODZIEWICZ**
WYKORZYSTANIE INFORMACJI O ROZMIESZCZENIU BUDYNKÓW DO ZARZĄDZANIA ZASOBAMI KOMUNIKACJI BEZPOŚREDNIEJ . . . . . 344

**F. MARZUK, A. VEJAR, P. CHOŁDA**
OPTIMAL RESOURCE ALLOCATION FOR 6G V2X COMMUNICATION SYSTEMS. . . . . 349

**W. KARCZ**
WPŁYW NORMY IEC 62232 I OCENY ZGODNOŚCI NA EFEKTYWNOŚĆ REALIZACJI INWESTYCJI RADIOKOMUNIKACYJNYCH . . . . . 352

## ST18. SYSTEMY I SIECI RADIOKOMUNIKACYJNE DLA ZASTOSOWAŃ SPECJALNYCH

**S. JANJI**
DEPLOYING AN AERIAL RECONFIGURABLE INTELLIGENT SURFACE FOR VEHICLE-TO-VEHICLE COMMUNICATIONS. . . . . 359

**M. KONIECZKA, P. SKOKOWSKI**
OCENA ZASTOSOWANIA BSP W PROCESIE MONITOROWANIA WIDMA W WALCE RADIOELEKTRONICZNEJ . . . . . 363

**B. BOSSY, G. FOTYGA, A. NOWAK, P. ŻUKOWSKI**
REKURENCYJNY ALGORYTM DETEKCJI SYGNAŁU . . . . . 367

**J. GAJEWSKI, J. ŁOPATKA**
ZAAWANSOWANE METODY LOKALIZACJI URZĄDZEŃ NADAWCZYCH W TERENIE ZURBANIZOWANYM . . . . . 372

## ST19. SYSTEMY I SIECI RADIOFONICZNE, TELEWIZYJNE I SATELITARNE

**J. PIELESZEK, K. BRÓDKA**
CZY KONIEC RADIOFONII UKF-FM JEST BLISKI . . . . . 376

**I. MICHALSKI, R. ZIELIŃSKI**
PORÓWNANIE CHARAKTERYSTYK ZANIKÓW W JEDNOCZĘSTOTLIWOŚCIOWEJ SIECI DAB+ SYMULOWANYCH I ZMIERZONYCH . . . . . 380

**M. SYBIS, W. FLAKOWSKI, M. RODZIEWICZ, R. KRENZ**
NAZIEMNA STACJA DO KOMUNIKACJI SATELITARNEJ W PASMACH UHF/VHF/S/X/C . . . . . 384

**K. KOSTRZEWSKA, P. KRYSZKIEWICZ**
MODELOWANIE NIELINIOWEJ CHARAKTERYSTYKI SZEROKOPASMOWYCH WZMACNIACZY RADIOWYCH O ZMIENNYM NAPIĘCIU ZASILANIA. . . . . 388

## ST20. KOMPRESJA WIZJI

**M. KACZYŃSKI, Z. PIOTROWSKI**
LUSTRZANY KODEK VIDEO BAZUJĄCY NA GŁĘBOKIEJ SIECI NEURONOWEJ . . . . . 396

**J. SAMELAK**
PREDICTION TECHNIQUES FOR COMPRESSION OF MULTIVIEW VIDEO ACQUIRED USING SYSTEMS WITH VARIOUS CAMERAS . . . . . 400

**F. KORUS, D. JUSZKA, M. GREGA, M. LESZCZUK, M. SUCHOŃ**
WYKRYWANIE TRUDNYCH DO KOMPRESJI SEKWENCJI WIDEO NA PODSTAWIE OBIEKTYWNYCH METRYK JAKOŚCI. . . . . 404

## ST21. ROZWIĄZANIA DLA SYSTEMÓW I SIECI CHMUROWYCH

**W. TEKIELA, J. DOMŻAŁ**
AUTOMATYCZNE GENEROWANIE ŚRODOWISK TESTOWYCH W SYSTEMIE ZARZĄDZANIA ZMIANĄ W SIECIACH. . . . . 408

**J. MARTYNA**
RÓWNOWAŻENIE OBCIĄŻEŃ I OPÓŹNIEŃ W ARCHITEKTURZE CHMUR BRZEGOWYCH DLA OBLICZEŃ MOBILNYCH . . . . . 413

**D. DULAS, J. WITULSKA, A. WYŁOMAŃSKA, K. WALKOWIAK**
MODEL OPARTY NA DANYCH DO DŁUGOTERMINOWEGO PROGNOZOWANIA PRZEPUSTOWOŚCI I OPÓŹNIEŃ PLASTRÓW SIECI 5G Z KONTEKSTEM KONFIGURACJI KOMÓRKI. . . . . 418

DOI: 10.15199/59.2024.4.1

# Cyberbezpieczeństwo: jasne i ciemne strony współczesnych technologii

## Cybersecurity: The Bright and Dark Sides of Today's Technologies

STRESZCZENIE Artykuł porusza zagadnienia związane z cyberbezpieczeństwem we współczesnym świecie, ukazując zarówno pozytywne, jak i negatywne aspekty nowoczesnych technologii. Autorzy opisują główne zagrożenia w cyberprzestrzeni, takie jak złośliwe oprogramowanie, ataki hakerskie, naruszenia prywatności oraz technologie deepfake. Przedstawiono przykłady technologii, które mogą być wykorzystywane w sposób zarówno konstruktywny, jak i destrukcyjny. Podkreślono znaczenie rozwoju sztucznej inteligencji i uczenia maszynowego w doskonaleniu środków bezpieczeństwa, jednocześnie zwracając uwagę na nowe wyzwania, jakie te technologie przynoszą. Artykuł akcentuje także konieczność edukacji oraz zwiększania świadomości w zakresie cyberbezpieczeństwa, zwłaszcza w kontekście współpracy międzysektorowej i adaptacji programów nauczania do dynamicznie zmieniających się wymagań rynku. Przedstawiono rolę zaawansowanych technologii, takich jak blockchain i kryptografia kwantowa, w kontekście przyszłych zagrożeń oraz potrzebę wprowadzenia nowych, odpornych na ataki systemów zabezpieczeń. Autorzy podkreślają również, że kluczowe jest znalezienie równowagi między środkami bezpieczeństwa a prawem do prywatności oraz nieustanne dostosowywanie strategii ochrony do szybko ewoluującego krajobrazu zagrożeń technologicznych i geopolitycznych.
SŁOWA KLUCZOWE: cyberbezpieczeństwo, ochrona prywatności, sztuczna inteligencja, kryptografia, blockchain, technologie kwantowe, przetwarzanie języka naturalnego, DDoS, deepfake

ABSTRACT The article discusses issues related to cybersecurity in the modern world, highlighting both the positive and negative aspects of contemporary technologies. The authors describe major threats in cyberspace, such as malware, hacking attacks, privacy breaches, and deepfake technologies. Examples of technologies that can be used in both constructive and destructive ways are presented. The importance of the development of artificial intelligence and machine learning in improving security measures is emphasized, while also noting the new challenges these technologies bring. The article also underscores the necessity of education and raising awareness in the field of cybersecurity, especially in the context of cross-sector collaboration and the adaptation of educational programs to the dynamically changing market demands. The role of advanced technologies such as blockchain and quantum cryptography in the context of future threats and the need for implementing new, attack-resistant security systems is discussed. The authors also stress that it is crucial to find a balance between security measures and the right to privacy, as well as to continuously adapt protection strategies to the rapidly evolving landscape of technological and geopolitical threats.
KEYWORDS cybersecurity, privacy protection, artificial intelligence, cryptography, blockchain, quantum technologies, natural language processing, DDoS, deepfakeBragg gratings, critical infrastructure, structural health monitoring

dr hab. inż. GRZEGORZ BOROWIK, prof. NASK-PIB Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, Warszawa
https://orcid.org/0000-0003-4148-4817
borowik.grzegorz@gmail.com

dr inż. ANNA FELKNER[1],
https://orcid.org/0000-0003-3813-4840
anna.felkner@nask.pl

dr inż. ADAM KOZAKIEWICZ[2],
https://orcid.org/0000-0002-1377-5046
adam.kozakiewicz@nask.pl

[1] Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, Warszawa

CISA (*Cybersecurity and Infrastructure Security Agency*) [1] definiuje cyberbezpieczeństwo jako sztukę ochrony sieci, urządzeń i danych przed nieautoryzowanym dostępem lub wykorzystaniem w celach przestępczych oraz praktykę zapewniania poufności, integralności i dostępności informacji; inne definicje można znaleźć tutaj [2]. W związku z tym, że obecnie w dużej mierze „żyjemy" w sieci internetowej, cyberbezpieczeństwo staje się ważniejsze niż kiedykolwiek do tej pory.

W cyberprzestrzeni istnieje wiele różnych zagrożeń, które mogą wpływać na bezpieczeństwo i prywatność użytkowników oraz organizacji. Niektóre z głównych zagrożeń to:

- Malware, czyli złośliwe oprogramowanie, takie jak wirusy, trojany, ransomware, czy keyloggery, stanowi duże zagrożenie dla systemów komputerowych i danych. Może prowadzić do kradzieży informacji, szkód finansowych, wizualnych czy też naruszenia prywatności.
- Ataki hakerskie, ataki wolumetryczne obciążające sieć internetową, takie jak DDoS (ang. *Distributed Denial of Service*), ataki typu phishing, ataki man-in-the-middle czy ataki na aplikacje webowe. Ich celem może być kradzież danych, przechwycenie kontroli nad systemem lub jego przeciążenie czy wykorzystanie systemu do dalszych ataków, np. ataki odbiciowe.
- Naruszenie prywatności poprzez na przykład wycieki danych, złamanie poufności informacji, śledzenie użytkowników i nadużycie danych osobowych.
- Socjotechniki, w ramach których atakujący wykorzystują manipulację psychologiczną i inne oszustwa, aby uzyskać dostęp do poufnych informacji. Poprzez wyrafinowane techniki psychologiczne, takie jak podszywanie się pod zaufane osoby, wykorzystanie zaufania lub

wprowadzanie w błąd, atakujący mogą nakłonić użytkowników do ujawnienia swoich danych lub wykonywania niebezpiecznych działań.
- Technologie deepfake, które umożliwiają manipulację treściami multimedialnymi, takimi jak audio, zdjęcia i filmy, w taki sposób, że są one trudne do odróżnienia od rzeczywistych. Może to prowadzić do rozprzestrzeniania dezinformacji, szantażu, fałszywych informacji czy naruszenia reputacji [3].

Ponadto, biorąc pod uwagę rosnącą skalę użycia sztucznej inteligencji (AI), zarówno zagrożenia jak i możliwości ich stosowania ewaluują w wielu różnych kierunkach.

Rozwój nowoczesnych technologii przyniósł zarówno pozytywne, jak i negatywne konsekwencje w obszarze cyberbezpieczeństwa [4]. Do pozytywnych należy zaliczyć między innymi ulepszone środki bezpieczeństwa, ponieważ postęp technologiczny umożliwił opracowanie solidnych rozwiązań w zakresie cyberbezpieczeństwa, takich jak zaawansowane techniki szyfrowania, uwierzytelnianie biometryczne [5] i systemy wykrywania zagrożeń oparte na sztucznej inteligencji. Środki te pomagają chronić wrażliwe dane i systemy przed cyberzagrożeniami. Nowoczesne technologie, takie jak analiza dużych zbiorów danych i uczenie maszynowe, pozwalają na analizę ogromnych ilości danych, umożliwiając identyfikację potencjalnych zagrożeń cybernetycznych i wzorców ataków.

Bezpieczne kanały komunikacji, ułatwione dzięki zaawansowanym środkom cyberbezpieczeństwa, umożliwiły globalną łączność i współpracę, sprzyjając wzrostowi gospodarczemu oraz wymianie kulturowej. Skuteczne środki cyberbezpieczeństwa odgrywają kluczową rolę w zapewnieniu nieprzerwanego działania infrastruktury krytycznej, zapobiegając potencjalnie katastrofalnym zakłóceniom.

Ponadto, rosnące zapotrzebowanie na specjalistów ds. cyberbezpieczeństwa stworzyło szerokie możliwości kariery zawodowej, jednocześnie napędzając innowacje w tej branży. Rozwój technologii oraz ciągła ewolucja zagrożeń wymuszają na sektorze cyberbezpieczeństwa nieustanne dostosowywanie się do nowych wyzwań, co prowadzi do dynamicznego rozwoju narzędzi i metod ochrony.

Należy również uwzględnić szereg negatywnych aspektów związanych z zastosowaniem nowoczesnych technologii w kontekście cyberbezpieczeństwa. Przykładowo, poważne zagrożenie stanowi zwiększona powierzchnia ataku. Rozprzestrzenianie się połączonych urządzeń Internetu Rzeczy zwiększyło liczbę punktów dostępu, które cyberprzestępcy wykorzystują do ataków, eksploatując luki w zabezpieczeniach.

Dodatkowo, cyberprzestępcy coraz częściej wykorzystują sztuczną inteligencję i uczenie maszynowe do automatyzacji i zwiększania swoich możliwości, co utrudnia wykrywanie i obronę przed wyrafinowanymi zagrożeniami. Z kolei rygorystyczne środki bezpieczeństwa, takie jak nadzór użytkowników i praktyki gromadzenia danych, mogą naruszać prawa do prywatności, budząc obawy etyczne i prawne.

## PRZYKŁADOWE ZAGROŻENIA WYNIKAJĄCE Z ROZWOJU TECHNOLOGICZNEGO

### Deepfake i jego wpływ na bezpieczeństwo informacji

Poważnym i wieloaspektowym zagrożeniem, jakie stwarza dla społeczeństwa szybki rozwój technik AI, jest technologia deepfake, czyli wykorzystanie sieci neuronowych do wytwarzania wizerunków nieistniejących osób lub fałszowanie wizerunków osób istniejących [6]. Wprawdzie zjawisko fałszowania w różnych celach zdjęć czy nagrań jest starsze od komputerów (montaż audio, retusz fotografii, malarstwo hiperrealistyczne), skala zjawiska zawsze była ograniczona przez pracochłonność manualnej obróbki materiałów, nawet przy wykorzystaniu nowoczesnych narzędzi komputerowych. Wykorzystanie technik sztucznej inteligencji pozwala jednak tworzyć fałszywe materiały dobrej jakości w krótkim czasie i niewielkim kosztem. Kluczowa jest różnica w samej metodzie, gdzie zamiast mozolnego i ograniczonego dostępnym materiałem dopasowywania i edycji, wystarczy zgromadzić zestaw danych uczących wyglądu i/lub głosu odpowiedniej osoby i wygenerować pożądany obraz lub nagranie na podstawie wzorca lub jego specyfikacji – to oczywiście uproszczenie, jednak dobrze oddające kierunek rozwoju technologii.

Technologia ta ma oczywiście wiele pozytywnych zastosowań. W przemyśle filmowym pozwala nakręcić sceny z udziałem niedostępnych bądź nawet nieżyjących aktorów lub historycznych postaci, a także np. odmłodzić lub postarzyć je według potrzeb w sposób potencjalnie bardziej przekonujący, niż pozwala na to charakteryzacja i triki filmowe. Nieistniejące osoby mogą nadać ludzką twarz wizualizacjom dowolnej treści bez wiązania ich z żadną osobą, co w wielu kontekstach może być pożądane. Nie dziwi też popyt na usługę ożywienia starych zdjęć, które często są jedyną pamiątką po bliskich. Oczywiście każdy z tych przypadków użycia rodzi pewne trudności (choćby prawo do wizerunku, czy rynek pracy aktorów), jednak są to raczej aktualne i przyszłe wyzwania dla społeczeństwa niż zagrożenia. Niestety, zastosowań jawnie szkodliwych również nie brakuje, przy czym wiele z nich ma bardzo poważne skutki społeczne.

Możliwość przekonującej zmiany tożsamości postaci w obrazie lub wideo na inną, bądź wręcz wygenerowania dowolnej sceny z udziałem wybranej osoby może być oczywiście zrealizowana również bez zgody tej osoby. Konsekwencje takiego użycia mogą być różne, zarówno w sensie namacalnym (ekonomicznym, prawnym), jak i psychologicznym [7]. Traumatyczne może być wykorzystanie tej techniki do tworzenia kompromitujących materiałów, wystarczająco przekonujących, aby spowodować poważne konsekwencje wizerunkowe, co znajduje zastosowanie zarówno w polityce, jak i w życiu codziennym, np. w sprawach rozwodowych. Materiały takie bywają tworzone nie tylko w celu skompromitowania danej osoby, przeprowadzenia szantażu, czy włożeniu w jej usta nieprawdziwych wypowiedzi – ludzkie instynkty niezawodnie prowadzą do wyko-

rzystania tej techniki do celów erotycznych, od częściowego rozebrania znanych postaci czy własnych znajomych na istniejących zdjęciach, po produkcję realistycznych materiałów o charakterze stricte pornograficznym, ograniczonych jedynie wyobraźnią twórcy. Nietrudno sobie wyobrazić, jak traumatyczne może być takie wykorzystanie wizerunku dla ofiary. Temat deepfake pojawia się też w kontekście materiałów CSAM (*Child Sexual Abuse Material*) – w tym przypadku problemem jest nie tylko wykorzystanie wizerunku dziecka w sposób podobny do wyżej wymienionych, ale także wytwarzanie takich materiałów z nieistniejącymi dziećmi. W świetle prawa posiadanie materiałów o tym charakterze jest karalne niezależnie od faktycznego istnienia ofiary.

Warto zaznaczyć, że destrukcyjny charakter ma nie tylko użycie technik deepfake, ale i sama możliwość łatwego tworzenia fałszywych treści – podważa ona bowiem zaufanie do wszelkich materiałów cyfrowych. Może to tyczyć się zarówno zwykłych wiadomości, czy innych materiałów dostępnych w sieci, jak i materiału dowodowego w postępowaniach sądowych. Fałszowanie dowodów, czy też ukrywanie faktycznych dowodów w gąszczu podobnych, ale fałszywych, nie jest jedynie narzędziem dezinformacji. Rozwój technik deepfake, w szczególności coraz trudniejsze wykrywanie fałszerstw, stanowi poważne wyzwanie dla wymiaru sprawiedliwości.

Łatwość tworzenia fałszywych materiałów z użyciem prawdziwego wizerunku wybranej osoby czyni z technik deepfake doskonałe narzędzie dla oszustów. Znane sposoby oszustw „na wnuczka" stają się znacznie groźniejsze, gdy „wnuczek" może posługiwać się realistyczną kopią prawdziwego głosu osoby, pod którą się podszywa. Duże wymagania obliczeniowe na razie ograniczają możliwość przeprowadzenia podobnego ataku z użyciem połączeń wideo – do płynnej rozmowy niezbędna byłaby generacja przekonującego obrazu zsynchronizowanego z dźwiękiem w czasie niemal rzeczywistym. Niemniej trzeba przyznać, że oszustwa takie mogą być jeszcze bardziej przekonujące od telefonicznych, a przy tym nie ma powodu, by uznać takie ataki w przyszłości za trwale niemożliwe, zwłaszcza przy oszustwach na duże kwoty, uzasadniających dużą inwestycję w przygotowania i moc obliczeniową. Choć rozmowy na żywo z oszustem prezentującym się na wideo jako inna osoba to jeszcze raczej pieśń – być może nieodległej – przyszłości, to wygenerowane w ten sposób wideo może być wykorzystane do oszustwa już dziś, choć bez możliwości interakcji. Należy podkreślić, że już teraz w co najmniej jednym udokumentowanym przypadku doprowadziło to do wielomilionowych strat w wyniku wysłania przez pracownika dużego przelewu na podstawie bezpośredniego, wyraźnego i realistycznego, ale sfałszowanego polecenia przełożonego przekazanego „ustnie" w przesłanym nagraniu wideo. Jedynie ścisłe trzymanie się dobrze opracowanych procedur wymagających odpowiedniego obiegu dokumentów i wiarygodnych podpisów cyfrowych może stanowić skuteczne zabezpieczenie przed takimi atakami w czasach, gdy coraz większa część interakcji w firmach odbywa się zdalnie.

Powyższe zagrożenia stawiają przed społeczeństwem wiele wyzwań, organizacyjnych i prawnych, takich jak pomoc ofiarom, skuteczne ściganie, minimalizacja negatywnych skutków. Od strony technologicznej istotne jest właściwie jedno pytanie – czy potrafimy skutecznie odróżniać deepfake od prawdziwych obrazów i czy możemy ufać, że tak pozostanie? Badania wskazują, że samoocena zdolności odróżniania obrazów prawdziwych od sztucznych już dziś jest powszechnie znacznie zawyżona [8]. Jesteśmy często przekonani, że pomyłki są raczej skutkiem nieuwagi i przy uważnym przyjrzeniu się deepfake jest łatwy do rozpoznania. W faktycznych testach jednak ludzka sprawność w tym zadaniu rozczarowuje – co prawda wyniki są lepsze od losowych, czyli przynajmniej w części przypadków potrafimy zauważyć różnice, jednak poziom błędów jest bardzo niepokojący, zwłaszcza, że metody deepfake nadal się rozwijają. Tym ważniejszym wyzwaniem technicznym jest opracowywanie skutecznych metod wykrywania fałszerstw, zarówno w formie zautomatyzowanej, przeznaczonej do szerokiego stosowania, jak i w formie narzędzi dla ekspertów, poprawiających wiarygodność ich orzeczeń w szczególnie istotnych przypadkach.

Pytanie o przyszłą możliwość wykrywania najbardziej zaawansowanych deepfake'ów pozostaje otwarte. Wysoka aktywność badaczy na tym polu daje nadzieję, że jeszcze w najbliższych latach detekcja deepfake będzie możliwa z zadowalającą skutecznością co najmniej przy dogłębnej analizie. Gama proponowanych technik jest bardzo szeroka [9, 10]. Pod uwagę brane są różne cechy badanego materiału – zarówno cechy samego obrazu lub dźwięku, jak i np. cechy biometryczne występujących w nim osób. Metody analizy sięgają od klasycznych metod statystycznych, poprzez rozmaite algorytmy uczenia maszynowego, po głębokie uczenie. Proponowane są także różne metody potwierdzania autentyczności materiałów, w szczególności duże zainteresowanie budzi tu wykorzystanie technologii blockchain.

Pocieszający jest fakt, że w przypadku większości wymienionych zastosowań pogoń za doskonałym ukryciem nie jest potrzebna. Odporność na najbardziej zaawansowane metody wykrywania potrzebna jest jedynie przy fałszowaniu dowodów do postępowań sądowych, ewentualnie przy opracowywaniu materiałów do najbardziej ambitnych i wysokobudżetowych prób szantażu czy dezinformacji. W większości przypadków wystarczy odporność na mniej zaawansowane metody stosowane masowo w automatycznych filtrach oraz nieodróżnialność przez większość odbiorców – samo dotarcie do grupy docelowej wystarcza by zasiać wątpliwości. W końcu w niektórych przypadkach (np. erotyka) odporność na metody detekcji jest zupełnie nieistotna, ważne jest jedynie to, aby zminimalizować widoczne gołym okiem niedoskonałości.

## NARUSZENIE BEZPIECZEŃSTWA DANYCH PRZY UŻYCIU TECHNOLOGII OMG CABLE

Przykładem technologii, która może być wykorzystywana w sposób szkodliwy lub niezamierzony jest technologia OMG, będąca zaawansowaną wersją standardowego

kabla USB. Jest on narzędziem wykorzystywanym głównie do testów bezpieczeństwa, np. w testach penetracyjnych, ale również do przeprowadzania ataków typu „man-in-the-middle". Tym samym kabel OMG może prowadzić do poważnych naruszeń bezpieczeństwa danych, w szczególności może być użyty do przechwytywania poufnych informacji przesyłanych między komputerem a urządzeniami peryferyjnymi, takimi jak klawiatury czy pendrive'y. Dzięki wbudowanym modułom bezprzewodowym, osoba używająca takiego kabla może zdalnie monitorować wszystkie wprowadzane dane, w tym hasła, dane logowania oraz treści wiadomości. Ponadto, kabel OMG może być wykorzystany do wprowadzenia złośliwego oprogramowania na urządzenie ofiary. Automatyczne uruchamianie skryptów instalujących trojany, wirusy lub inne formy złośliwego oprogramowania może prowadzić do utraty danych, szpiegowania lub uzyskania nieautoryzowanego dostępu do systemu.

Kabel umożliwia zdalne monitorowanie aktywności użytkownika, na przykład poprzez rejestrowanie klawiatury, co pozwala na śledzenie wszystkich działań ofiary na komputerze. Inwigilacja może być prowadzona bez wiedzy i zgody, co stanowi poważne naruszenie prywatności. Dodatkowo, dzięki możliwości zdalnego sterowania, atakujący mogą uzyskać dostęp do poufnych danych przechowywanych na komputerze. Może to obejmować dokumenty, e-maile, zdjęcia oraz inne wrażliwe informacje, które następnie mogą być wykorzystane do szantażu, kradzieży tożsamości lub innych nieuczciwych działań.

Technologia OMG stwarza również zagrożenie dla bezpieczeństwa infrastruktury IT w organizacjach. Atakujący mogą podłączyć kabel do komputerów firmowych, aby uzyskać dostęp do sieci korporacyjnej, co w konsekwencji prowadzi do kradzieży danych, sabotażu systemów informatycznych lub innych form cyberataków. Użytkownicy indywidualni, którzy nie są świadomi istnienia kabla OMG, mogą paść ofiarą ataków prowadzonych przez osoby trzecie. Atakujący mogą łatwo wymienić standardowy kabel USB na OMG w miejscach publicznych, takich jak kawiarnie, biblioteki czy lotniska. Świadomość istnienia takich zagrożeń oraz stosowanie odpowiednich środków ostrożności są więc kluczowe aby zminimalizować ryzyko związane z potencjalnym atakiem.

## DDOS JAKO NARZĘDZIE CYBERATAKÓW

Zaawansowane narzędzia i techniki, takie jak sztuczna inteligencja i uczenie maszynowe, znacząco wzmacniają systemy obronne, pozwalając na szybsze i skuteczniejsze wykrywanie oraz neutralizowanie zagrożeń. Jednakże, te same technologie mogą być wykorzystywane przez cyberprzestępców do przeprowadzania coraz bardziej złożonych i trudnych do wykrycia ataków. Przykładem takiego zjawiska są ataki typu Denial of Service (DoS), które, mimo że są dobrze znane w świecie cyberbezpieczeństwa, wciąż stanowią poważne zagrożenie dla stabilności i dostępności usług sieciowych.

Atak typu Denial of Service (DoS) jest jednym z najgroźniejszych rodzajów cyberataków, którego celem jest zablokowanie lub pogorszenie jakości usług sieciowych. Najczęstszą formą tego ataku jest Distributed Denial of Service (DDoS), wykonywany przez liczne urządzenia w sieci, często tworzące botnet. Ataki DDoS można podzielić na dwie główne kategorie: aplikacyjne i infrastrukturalne, które z kolei dzielą się na ataki bezpośrednie i odbiciowe. Ataki te stanowią poważne zagrożenie dla stabilności i dostępności usług internetowych, wpływając negatywnie na działalność zarówno przedsiębiorstw, jak i instytucji publicznych.

Ataki bezpośrednie obejmują ataki wolumetryczne, których celem jest przeciążenie łącza sieciowego poprzez wysłanie ogromnej liczby pakietów. Przykładami takich ataków są floody UDP i ICMP. Z kolei ataki odbiciowe wykorzystują podatności różnych usług, takich jak DNS i NTP, gdzie atakujący wysyła zapytania do serwerów z podmienionym adresem IP ofiary, generując w ten sposób wielokrotne obciążenie. Inną kategorią są ataki protokołowe, które wykorzystują podatności warstw L3 i L4. Przykłady to SYN Flood, atakujący mechanizm three-way handshake protokołu TCP, oraz Fragmentation Attack, wykorzystujący podatności oprogramowania związane z fragmentacją pakietów.

Ataki aplikacyjne, działające na warstwie L7, są szczególnie trudne do wykrycia, ponieważ wykorzystują specyficzne podatności aplikacji. Nawet niewielka ilość ruchu generowanego przez takie ataki może spowodować znaczne szkody. Do typowych przykładów należą Slowloris, R.U.D.Y. (R-U-Dead-Yet), oraz Slow Read Attack, które zakłócają normalne połączenia sieciowe, zapełniając tablice połączeń i uniemożliwiając dostęp do usługi. Według statystyk Cloudflare, liczba ataków na warstwy L3/L4 wzrosła o 85% w 2023 roku w porównaniu do roku 2022, co podkreśla rosnące zagrożenie i potrzebę ciągłego monitorowania oraz wprowadzania zaawansowanych środków ochrony przed tego typu atakami [11].

## BLOCKCHAIN I MIKSERY KRYPTOWALUT

Technologia blockchain, stanowiąca fundament kryptowalut takich jak Bitcoin, zrewolucjonizowała sposób przeprowadzania transakcji cyfrowych, oferując zdecentralizowaną, transparentną i niezmienną księgę rozliczeniową. Kluczowym aspektem tej technologii jest zapewnienie anonimowości i bezpieczeństwa transakcji, co czyni ją atrakcyjną nie tylko dla zwykłych użytkowników, ale i dla różnych podmiotów o mniej etycznych intencjach [12, 13].

Każda transakcja w sieci blockchain jest zapisywana w blokach, z których każdy jest chronologicznie i kryptograficznie połączony z poprzednim, tworząc łańcuch. Dzięki zastosowaniu funkcji hashujących oraz mechanizmów takich jak Proof of Work, blockchain gwarantuje niezmienność zapisów, co stanowi o jego wyjątkowej odporności na modyfikacje i ataki [14]. Anonimowość użytkowników jest zachowana przez pseudonimizację, gdzie zamiast danych osobowych użytkownika, transakcje są identyfikowane przez skomplikowane adresy kryptograficzne [15].

Miksery kryptowalut, czyli usługi umożliwiające mieszanie środków różnych użytkowników w celu zwiększenia pry-

watności, stanowią kolejny poziom zabezpieczenia anonimowości. Przez przesyłanie kryptowalut przez różne adresy i „mieszanie" ich z aktywami innych osób, miksery utrudniają śledzenie środków do oryginalnego źródła [16]. Choć ta metoda jest skuteczna w ochronie prywatności, rodzi też poważne pytania etyczne i prawne, zwłaszcza w kontekście możliwości wykorzystywania tych usług do prania pieniędzy czy finansowania nielegalnych działań [17].

Anonimowość i zdecentralizowana natura blockchaina mogą służyć nie tylko ochronie prywatności, ale również otwierają drogę dla działalności przestępczej. Organizacje przestępcze mogą wykorzystać te cechy do ukrywania nielegalnych transakcji i unikania odpowiedzialności prawnej [18, 19]. Przykładowo, Bitcoin odegrał znaczącą rolę w działalności rynku Silk Road, platformy internetowej, na której handlowano narkotykami i innymi nielegalnymi towarami [13].

W odpowiedzi na te wyzwania, organy ścigania na całym świecie intensyfikują wysiłki w zakresie rozwijania technologii i metod umożliwiających śledzenie transakcji kryptowalutowych. Narzędzia takie jak analiza blockchain pozwalają na identyfikację i śledzenie podejrzanych transakcji, co stanowi istotny krok w walce z przestępczością cyfrową [12, 20]. Pomimo tych działań, balans między ochroną prywatności a bezpieczeństwem pozostaje kluczowym wyzwaniem dla blockchaina i kryptowalut [14, 15].

## NOWOCZESNE TECHNOLOGIE A CYBERBEZPIECZEŃSTWO

### Sztuczna inteligencja w cyberbezpieczeństwie

Wprowadzenie technik uczenia maszynowego (ML) w obszarze cyberbezpieczeństwa przyniosło znaczące korzyści, jednocześnie stawiając przed nami nowe wyzwania. Arthur Samuel, który w 1959 roku zaproponował termin „uczenie maszynowe", opisał je jako zdolność komputerów do nauki bez konieczności ich bezpośredniego programowania. Dzięki tej zdolności, ML znajduje dziś zastosowanie w niemal każdej dziedzinie, w tym w sektorze opieki zdrowotnej, rekomendacji produktów, platformach społecznościowych, bankowości, cyberbezpieczeństwie, systemach nadzoru, prognozowaniu, grach, inteligentnych botach oraz polityce. W kontekście cyberbezpieczeństwa, ML może być skutecznym narzędziem, które analizuje ogromne ilości danych dotyczących zagrożeń, rozpoznaje wzorce i uczy się ich, aby zapobiec podobnym atakom w przyszłości. Uczenie maszynowe odgrywa kluczową rolę w rozwoju algorytmów przeciwdziałających phishingowi, systemów wykrywania włamań, systemów uwierzytelniania oraz systemów wykrywania oszustw internetowych.

Techniki uczenia maszynowego znacząco wpływają na rozwój systemów bezpieczeństwa, które potrafią adaptować się do zmieniających się zagrożeń i skutecznie chronić dane użytkowników przed coraz bardziej zaawansowanymi atakami [4]. W porównaniu z tradycyjnymi metodami obliczeniowymi, gdzie komputery muszą być precyzyjnie zaprogramowane, algorytmy ML uczą się bezpośrednio z danych, co pozwala na odkrywanie wartościowych informacji, nawet jeśli nie zostały one wcześniej zdefiniowane. Ta własność sprawia, że maszyny są dziś użyteczne w różnych dziedzinach, w tym w cyberbezpieczeństwie, które dąży do zapewnienia poufności, integralności i dostępności danych. Poufność zapobiega dostępowi nieautoryzowanych osób do wrażliwych danych, co chroni zasoby prywatne i zapewnia, że tylko upoważnieni pracownicy mają do nich dostęp. Integralność chroni dane przed manipulacją, utrzymując ich spójność i ważność, zaś dostępność gwarantuje, że dane są dostępne dla uprawnionych użytkowników zawsze, gdy są potrzebne. Wykorzystanie technik ML, takich jak klasyfikacja, regresja, klasteryzacja i rekomendacje, pozwala na efektywne wykrywanie zagrożeń, analizę behawioralną, uwierzytelnianie adaptacyjne oraz automatyzację zadań związanych z cyberbezpieczeństwem, co zwiększa skuteczność ochrony infrastruktury krytycznej i systemów informatycznych.

Sztuczna inteligencja (AI) oraz uczenie maszynowe mają szerokie zastosowanie w cyberbezpieczeństwie, oferując poprawę wydajności, szybkości i skuteczności reakcji na zagrożenia oraz zwiększenie ochrony przed atakami hakerskimi. Obszary, w których AI znajduje praktyczne zastosowanie, obejmują między innymi:

- wykrywanie podejrzanej aktywności, anomalii czy zagrożeń dzięki temu, że systemy AI mogą analizować duże ilości danych z różnych źródeł, takich jak logi zdarzeń, dane sieciowe czy dane dotyczące zachowań użytkowników - wykorzystując techniki uczenia maszynowego i analizę behawioralną, AI jest w stanie zidentyfikować nieznane wzorce i zachowania charakterystyczne dla ataków hakerskich;
- automatyzację reakcji na incydenty przyspieszającą wykrywanie, analizę i odpowiedź na ataki cybernetyczne – systemy AI mogą podejmować działania zapobiegawcze, takie jak blokowanie podejrzanych adresów IP, izolowanie zainfekowanych urządzeń czy generowanie alertów dla zespołów odpowiedzialnych za bezpieczeństwo;
- analizę logów i zdarzeń poprzez identyfikację wzorców, związki między zdarzeniami oraz wykrywanie nietypowych lub podejrzanych aktywności – możliwe jest szybsze wykrywanie incydentów i reagowanie na nie;
- identyfikację i analizę złośliwego oprogramowania, takiego jak wirusy, trojany czy ransomware, poprzez analizę kodu, zachowań aplikacji czy cech charakterystycznych dla szkodliwych programów - możliwe jest szybsze wykrywanie i reagowanie na złośliwe oprogramowanie;
- przewidywanie ataków dzięki temu, że AI może wykorzystać dane historyczne, analizę trendów i algorytmy przewidujące do identyfikacji potencjalnych zagrożeń i przewidywania przyszłych ataków - systemy AI mogą analizować dane dotyczące znanych zagrożeń i innych czynników, aby generować prognozy dotyczące przyszłych ataków i podejmować odpowiednie środki zapobiegawcze;
- weryfikację tożsamości i uwierzytelnianie, zarówno na podstawie tradycyjnych metod, jak i na podstawie analizy

biometrycznej, takiej jak rozpoznawanie twarzy czy analiza dźwięku - można zwiększyć bezpieczeństwo procesów uwierzytelniania i ograniczyć ryzyko nieautoryzowanego dostępu.

Metody uczenia maszynowego znajdują przykładowo zastosowanie w detekcji logowania się osób niepowołanych do aplikacji internetowych. Opracowane w [5] rozwiązanie stanowi przełom w metodach identyfikacji i zapobiegania nieautoryzowanemu dostępowi. Autorzy podkreślają, że wdrożenie ML do systemów uwierzytelniania wieloskładnikowego pozwala na wykrywanie nieprawidłowości w zachowaniu użytkowników, które wskazują na próbę przejęcia konta. Autorzy proponują szczegółową metodykę oceny systemów opartą na ML. Zastosowana analiza użycia klawiatury komputera (dynamiki naciśnięć klawiszy) przez obserwację zachowania użytkowników w czasie sesji, umożliwia ciągłe monitorowanie ich autentyczności. Modele ML trenowane były na różnych zbiorach danych, w tym na danych rzeczywistych pochodzących z aplikacji finansowych. Dzięki temu są odporne na różne metody działania oszustów. W badaniach wykazano, że odpowiednio zaprojektowane techniki, mogą skutecznie zredukować wskaźniki fałszywej akceptacji i błędnych odrzuceń, co potwierdza użyteczność zaproponowanego rozwiązania w zwiększaniu dokładności systemów ochrony aplikacji internetowych. Podejście nie tylko podnosi poziom bezpieczeństwa aplikacji internetowych, ale również przyczynia się do głębszego zrozumienia zachowania użytkowników. Rozwiązanie ma kluczowe znaczenie dla rozwoju systemów bezpieczeństwa, które potrafią adaptować się do zmieniających się zagrożeń i skutecznie chronić dane użytkowników przed coraz bardziej zaawansowanymi atakami.

## ODPOWIEDZIALNA AI I AI ALIGNMENT

W epoce rosnącej obecności sztucznej inteligencji w różnych aspektach życia i pracy, istotne staje się rozważanie i wdrażanie koncepcji odpowiedzialnej AI (Responsible AI) oraz jej zgodności z wartościami i celami społecznymi (AI Alignment). Znaczenie etycznych aspektów stosowania AI jest kluczowe dla budowania zaufania i akceptacji społecznej wobec tej technologii. Etyka w AI chroni przed negatywnymi skutkami jej stosowania oraz pomaga w maksymalnym wykorzystaniu jej potencjału dla wspólnego dobra. Rozwój odpowiedzialnych praktyk, polityk i standardów w zakresie AI jest więc niezbędny, aby zapewnić, że technologia będzie służyć człowiekowi w etyczny i konstruktywny sposób.

Dyskusja na temat odpowiedzialnej AI i AI Alignment jest coraz bardziej powszechna, a jej znaczenie rośnie w miarę dalszego rozwoju i implementacji technologii AI w różnych sektorach. Odpowiedzialna AI promuje rozwijanie i stosowanie technologii w sposób świadomy i etyczny, który uwzględnia potencjalne konsekwencje dla wszystkich zainteresowanych stron. Podejście wymaga, aby algorytmy były sprawiedliwe, nie wprowadzały dyskryminacji i były wolne od stronniczości. Przykładowo, organizacje używające AI do celów rekrutacji powinny upewnić się, że ich systemy nie dyskryminują kandydatów na podstawie płci, rasy czy wieku.

Transparentność sztucznej inteligencji oznacza, że systemy powinny być zrozumiałe dla użytkowników, a decyzje podejmowane przez AI możliwe do prześledzenia i zrozumienia. Wdrażane przez projektantów systemów metody, muszą umożliwiać użytkownikom zrozumienie, na jakiej zasadzie AI podejmuje decyzje. Istotne jest, aby algorytmy mogły być kontrolowane, a ich działania podlegały audytom, co zwiększa zaufanie użytkowników. AI powinna być projektowana w sposób, który minimalizuje ryzyko niezamierzonych konsekwencji, takich jak niecelowa dezinformacja. Kluczowe jest więc ciągłe monitorowanie systemów AI oraz identyfikacja i korygowanie błędów, które mogą prowadzić do generowania fałszywych informacji lub nieprawidłowych danych. AI Alignment skupia się na zgodności działania systemów AI z wartościami i celami społecznymi, takimi jak poprawa jakości życia, zwiększanie efektywności i promowanie dobrobytu, przy jednoczesnym unikaniu działań szkodliwych. Wyzwaniem jest tu definiowanie i wdrażanie tych wartości w sposób, który jest akceptowany przez różnorodne grupy społeczne.

Generowanie automatycznych treści przez modele językowe AI, mimo swojego potencjału w usprawnianiu dostępu do informacji i procesów komunikacyjnych, rodzi poważne wyzwania związane z niezamierzonymi błędami oraz manipulacjami. Można łatwo wskazać dualne zastosowanie nowoczesnych technologii, które oprócz korzyści mogą być wykorzystywane do celów cyberprzestępczych, w tym dezinformacji. Niecelowa dezinformacja pojawia się często jako produkt błędów w algorytmach AI, które nie potrafią właściwie zrozumieć kontekstu ludzkiego języka i generują treści mogące wprowadzać w błąd [21]. Problem ten jest szczególnie istotny w kontekście bezpieczeństwa narodowego, gdzie precyzyjna i wiarygodna komunikacja jest kluczowa.

Istotnym aspektem korzystania z technologii AI, szczególnie w kontekście bezpieczeństwa informacji, jest potrzeba wprowadzenia odpowiednich regulacji oraz przestrzegania etyki. Modelowanie językowe AI może być wykorzystywane do manipulowania opinią publiczną, co wymaga odpowiednich środków zaradczych i regulacji. W raporcie ENISA (2023) podkreślono konieczność stosowania filtrów tematycznych i międzynarodowej współpracy w celu ustalenia standardów ograniczających nadużycia w tej technologii [22]. Dążenie do przejrzystości i zrozumienia procesów AI, zgodnie z zaleceniami ISO/IEC 38507:2022, stanowi kluczowy element w budowaniu zaufania i odpowiedzialnego wykorzystania AI [23].

W kontekście bezpieczeństwa narodowego, manipulacja i błędy generowane przez AI mogą mieć poważne konsekwencje. Przykładem jest możliwość wykorzystania AI do tworzenia wiarygodnych fałszywych informacji, które mogą destabilizować systemy polityczne lub społeczne. Rozwój narzędzi opartych na AI, takich jak model GPT-X.Y i Bing Chat, wymaga zatem stałego monitorowania i aktualizacji w celu zapobiegania ich wykorzystaniu w działaniach szkodliwych. Wdrażanie restrykcji w czasach kryzysów, jak sugeruje ISO/IEC 27001:2022, może być niezbędne dla ochrony integralności informacyjnej i bezpieczeństwa państwa [24].

Zastosowanie sztucznej inteligencji wiąże się więc z wieloma wyzwaniami i zagrożeniami. Należą do nich między innymi:

- etyka i prywatność, ponieważ wprowadzanie AI w różne dziedziny, takie jak analiza danych, monitorowanie zachowań, czy rozpoznawanie twarzy, może rodzić obawy dotyczące naruszenia prywatności, dyskryminacji czy nadużywania technologii;
- błędy i nietrafne decyzje w przypadku nieodpowiednio skonfigurowanych systemów AI, wykrywanie i odpowiedź na zagrożenia może być niewystarczające lub niewłaściwe;
- manipulacja i ataki na AI, w których atakujący mogą próbować wprowadzać fałszywe dane, wpływać na decyzje podejmowane przez systemy AI lub próbować obejść ich zabezpieczenia;
- brak transparentności, zwłaszcza w przypadku niektórych głębokich sieci neuronowych znanych jako „czarne skrzynki", ich decyzje i procesy podejmowania decyzji są trudne do zrozumienia i wyjaśnienia. Brak transparentności może rodzić obawy dotyczące odpowiedzialności, sprawiedliwości i zaufania do systemów AI.

Wyzwania te mogą zostać zaadresowane i rozwiązane dzięki wypracowaniu odpowiednich środków obrony i wprowadzeniu zabezpieczeń, takich jak m.in. regularne aktualizacje, monitoring bezpieczeństwa i przestrzeganie najlepszych praktyk.

## ZASTOSOWANIE PRZETWARZANIA JĘZYKA NATURALNEGO W DETEKCJI OSZUSTW CYFROWYCH

Przetwarzanie języka naturalnego (NLP) jest coraz częściej wykorzystywane w systemach detekcji oszustw cyfrowych, w tym phishingu, dzięki swojej zdolności do analizowania i interpretowania ludzkiego języka na dużą skalę. Technologie NLP mogą identyfikować podejrzane wzorce w komunikacji i wyłapywać subtelne anomalie w treściach, które mogłyby zostać przeoczone przez tradycyjne metody. W [25] opisano zastosowanie uczenia maszynowego w identyfikacji stron phishingowych, gdzie modele NLP analizują słowa kluczowe i struktury językowe typowe dla oszukańczych wiadomości. Poprzez trenowanie na historii znanych ataków phishingowych, systemy te mogą z dużą efektywnością przewidywać i neutralizować próby oszustwa przed ich realizacją.

Rozwój NLP umożliwia nie tylko wykrywanie, ale również automatyczne reagowanie na potencjalne zagrożenia cybernetyczne. Zastosowanie zaawansowanych algorytmów NLP, takich jak te opisane w [26], umożliwia analizę zachowań użytkowników i ich zapytań w celu wykrywania niekonwencjonalnych prób dostępu lub nieautoryzowanych działań. Systemy te, wykorzystując analizę semantyczną i kontekstową, są w stanie dostarczać bardziej złożone i granularne rozwiązania bezpieczeństwa, które adaptują się do ewoluujących taktyk przestępców.

Mimo obiecujących wyników, implementacja NLP w cyberbezpieczeństwie niesie za sobą wyzwania, takie jak potrzeba ciągłego dostosowywania modeli do nowych metod i schematów oszustw, które dynamicznie się zmieniają. Jak zauważono w [27], skuteczność systemów detekcji opartych na NLP zależy od jakości i aktualności danych uczących, co wymaga regularnych aktualizacji i tzw. „dostrajania" modeli. Przyszłość NLP w cyberbezpieczeństwie będzie zatem zależała od zdolności do integracji z innymi technologiami i adaptacji do ciągle zmieniającego się krajobrazu zagrożeń cyfrowych.

## ZABEZPIECZENIA W KOMUNIKACJI MIĘDZY POJAZDAMI

Kluczowym elementem w rozwoju autonomicznych systemów transportowych jest zapewnienie bezpiecznej komunikacji między pojazdami (V2V) oraz między pojazdami a infrastrukturą (V2X). W kontekście ochrony, integralność i autentyczność przesyłanych komunikatów są niezbędne do zapewnienia wysokiego poziomu bezpieczeństwa i efektywności tych systemów. Protokoły takie jak IEEE 1609.2 i 3GPP TS 33.185 zalecają wykorzystanie infrastruktury klucza publicznego (PKI) do wzajemnego uwierzytelnienia i szyfrowania komunikacji między pojazdami, co zapewnia poufność i integralność danych. Jednakże, standardy te nie łączą cyfrowej tożsamości pojazdu z jego fizycznym stanem, co otwiera możliwość ataków przez tzw. „pojazdy duchy" [28].

Centralnym wyzwaniem w komunikacji V2V jest wiązanie tożsamości cyfrowej pojazdu z jego aktualnym stanem fizycznym, takim jak lokalizacja czy prędkość. Dzięki metodzie Proof-of-Following (PoF), przedstawionej w [28], możliwe jest zweryfikowanie, czy pojazd kandydujący rzeczywiście podąża za pojazdem weryfikującym w odpowiedniej odległości, bez konieczności ujawniania dokładnej lokalizacji. Technika ta wykorzystuje efekt dużej skali zanikania sygnału RF jako wspólnego źródła losowości, co jest kluczowe w ruchomym środowisku zewnętrznym, gdzie sygnał RF wykazuje szybką dekorelację zarówno w przestrzeni, jak i czasie. PoF pozwala na ochronę prywatności, jednocześnie uniemożliwiając zdalnym atakującym wpływanie na formacje pojazdów.

Implementacja PoF w realnych scenariuszach V2V i V2X może znacząco zwiększyć bezpieczeństwo komunikacji między pojazdami. Poprzez ograniczenie dostępu do sieci pojazdów tylko dla tych, które fizycznie uczestniczą w ruchu, metoda ta stanowi barierę dla ataków prowadzonych z odległych lokalizacji. Co więcej, potencjalne zastosowanie PoF w dynamicznych sieciach pojazdów, gdzie szybko zmieniające się warunki drogowe wymagają ciągłej weryfikacji tożsamości i stanu pojazdów, otwiera nowe możliwości dla rozwoju bezpiecznych systemów transportowych. Niezależnie od tego, kontynuacja badań nad PoF i jej integracja z istniejącymi standardami PKI może prowadzić do nowych standardów zabezpieczeń, które będą lepiej adresować specyficzne wyzwania stawiane przez autonomiczny transport [28].

## KRYPTOGRAFIA I KOMPUTERY KWANTOWE

Postępy w kryptografii kwantowej mogą stanowić potencjalne zagrożenie dla bezpieczeństwa kryptograficznego stosowanego obecnie w technologii opartej na block-

chain i innych systemach zabezpieczeń. Komputery kwantowe, zdolne do przetwarzania obliczeń na niespotykaną dotąd skalę, mogą łamać tradycyjne algorytmy kryptograficzne, takie jak RSA czy ECC (ang. *Elliptic Curve Cryptography*), w znacznie krótszym czasie. To rodzi potrzebę adaptacji do tzw. kryptografii postkwantowej, która wykorzystuje algorytmy odporne na ataki kwantowe, takie jak algorytmy oparte na problemach kratowych czy kodowych. Jak podaje Cybersecurity & Infrastructure Security Agency, przygotowanie do migracji na nowe standardy kryptograficzne jest kluczowe dla zapewnienia przyszłościowego bezpieczeństwa danych. ***„Government and critical infrastructure organizations must take coordinated preparatory actions now to ensure a fluid migration to the new post-quantum cryptographic standard that the National Institute of Standards and Technology (NIST) will publish in 2024" [37].***

Algorytmy oparte na problemach kratowych, takie jak Learning With Errors (LWE) i NTRU, stanowią obiecującą klasę algorytmów odpornych na ataki przy użyciu komputerów kwantowych. LWE, wprowadzony w 2005 roku, wykorzystuje złożoność obliczeniową związaną z problemami aproksymacyjnymi na strukturach kratowych, które są trudne do rozwiązania nawet przy użyciu zaawansowanych komputerów kwantowych. Z kolei NTRU, opracowany w 1996 roku, jest szybszym algorytmem kryptograficznym, który również opiera się na trudności znalezienia najkrótszego wektora w kratach. Oba te algorytmy oferują wysoki poziom bezpieczeństwa w obliczu rosnących możliwości komputerów kwantowych, co czyni je atrakcyjnymi dla zastosowań wymagających wysokiej odporności na ataki.

W dziedzinie kryptografii opartej na kodach, algorytmy takie jak McEliece z 1978 roku i Niederreiter z 1986 roku wykorzystują złożone struktury kodowania korekcyjnego błędów do tworzenia systemów kryptograficznych, które są trudne do złamania przez komputery kwantowe. Algorytmy bazują na trudności dekodowania ogólnych kodów liniowych, co stanowi solidną barierę dla potencjalnych ataków. Z kolei algorytmy wielomianowe, takie jak HFE (*Hidden Field Equations*) z 1996 roku oraz UOV (*Unbalanced Oil and Vinegar)* z 1999 roku, implementują skomplikowane równania wielomianowe, które są trudne do rozwiązania dla atakującego, co zapewnia bezpieczeństwo w współczesnym kontekście kryptograficznym.

Te zaawansowane techniki post-kwantowe są kluczowe dla przyszłości bezpieczeństwa cyfrowego, zwłaszcza w perspektywie rozwijającej się technologii kwantowej, która zagraża obecnym standardom kryptograficznym. Adaptacja tych metod w infrastrukturze cyfrowej i ich integracja z istniejącymi systemami to kluczowe kroki w zapewnieniu, że nasze dane pozostaną chronione w przyszłości, która będzie oparta na kwantowych możliwościach obliczeniowych.

## EDUKACJA I ŚWIADOMOŚĆ CYBERBEZPIECZEŃSTWA

Według raportu Koalicji IS3C „Closing the gap between the needs of the cybersecurity industry and the skills of tertiary education graduates" [29] istnieje wyraźna rozbieżność pomiędzy tym czego oczekuje biznes, a co daje uczelnia wyższa. Oznacza to, że należy przywiązywać większą wagę do sposobu, w jaki edukacja w zakresie cyberbezpieczeństwa jest prowadzona. W raporcie zwrócono uwagę na braki nie tylko w zakresie kompetencji zawodowych, typowych dla cyberbezpieczeństwa, takich jak zapobieganie ryzykom i zarządzanie ryzykami w zakresie ochrony Internetu, rozumienie zagadnień bezpiecznej komunikacji w Internecie i technologii internetowych, ale też niezwykle istotnych kompetencji przekrojowych, takich jak myślenie krytyczne, umiejętność rozwiązywania problemów, umiejętność pracy zespołowej czy kreatywność.

Z badań tych wynika, że respondenci z sektora biznesowo-przemysłowego przywiązywali około 10% większą wagę do umiejętności przekrojowych i zawodowych niż przedstawiciele sektora edukacyjnego. W wywiadach i w ankietach pojawiały się sugestie podkreślające, że grupa osób z sektora edukacji powinna bardziej skupić się na podstawach, takich jak pomaganie studentom w lepszym zrozumieniu działania systemów i aplikacji. Na podstawie badania sformułowano różnego rodzaju zalecenia, które obejmują między innymi poprawę współpracy międzysektorowej, modernizację procedur rekrutacyjnych w celu zwiększenia różnorodności oraz podnoszenie świadomości w celu zachęcenia użytkowników do przyjęcia bardziej odpowiedzialnego podejścia do własnego cyberbezpieczeństwa i zachęcenia większej liczby młodych ludzi do planowania kariery w tak szybko rozwijającym się sektorze gospodarki, jakim jest cyberbezpieczeństwo.

Jako pozytywny aspekt z tych badań można wyczytać, że zarówno sektor przemysłowo-biznesowy, jak i edukacyjny na całym świecie uznaje istnienie luki kompetencyjnej oraz wyraża podobne opinie na temat kluczowych w tym zakresie kompetencji. Zarówno uczelnie jak i biznes widzą potrzebę proponowania różnego rodzaju rozwiązań aby tę lukę zapełnić. Wśród rozwiązań proponowanych przez sektor biznesowy często przewijały się szkolenia, natomiast sektor uczelniany preferował współpracę i wymianę doświadczeń z biznesem w celu budowania realistycznych przyszłościowych programów nauczania.

Biorąc pod uwagę niewystarczającą ilość wykwalifikowanych pracowników na stanowiskach związanych z cyberbezpieczeństwem, niezwykle istotnym jest odpowiednie zmotywowanie ich do pracy. Ogólnie występują dwa rodzaje motywacji: wewnętrzna i zewnętrzna. Do wewnętrznej zaliczamy min. pragnienia, interesy, samorealizację, współpracę, zadowolenie, decyzyjność i zaufanie, natomiast zewnętrzna to np. zastraszanie, możliwość utraty pracy, obniżenie/podwyższenie pensji, awans/degradacja, przynęta czy możliwość rozwoju.

Firma PeopleKeys [30], zajmując się badaniami nad motywacją pracowników, zidentyfikowała sześć wewnętrznych motywacji, które przekładają się na wyniki.

- I – Wewnętrzny spokój (ang. *Inner Awareness/Spiritual*) – dążenie do spokoju, harmonii, działania w zgodzie ze swoimi wartościami;

- S – Solidarność (ang. *Social/Humanitarian*) – pragnienie pomocy innym;
- P – Wpływ (ang. *Power/Political*) – potrzeba wpływania na innych;
- E – Ekonomia (ang. *Economic/Tangible*) – dążenie do osiągania mierzalnych efektów, w tym finansowych;
- A – Artyzm (ang. *Artistic/Innovative*) – pragnienie wyrażania siebie, swojej kreatywności, indywidualizmu;
- K – Wiedza (ang. *Knowledge/Proficiency*) – potrzeba uczenia się, poznawania nowych rzeczy, rozumienia.

Niezwykle istotnym jest aby dążyć do zapewnienia wewnętrznych motywacji pracownikom.

Dbanie o cyberbezpieczeństwo to nie tylko kwestia technologii, ale także, a może przede wszystkim, czynnik ludzki. Tak zwane „*human-centric cybersecurity design*" zostało dostrzeżone jako jeden z najważniejszych aspektów projektowania cyberbezpieczeństwa już kilka lat temu. Obecnie ten trend się wzmacnia. W trendach na 2023 Gartner dostrzega to jako jeden z najważniejszych aspektów. Widoczna jest potrzeba równowagi pomiędzy ludźmi, procesami i technologią w celu skutecznego zmniejszenia ryzyka cyberbezpieczeństwa. Projektowanie cyberbezpieczeństwa skoncentrowanego na człowieku nadaje priorytet roli człowieka i jego doświadczenia a nie tylko rozwiązaniom technicznym. Opierając się na doświadczeniu użytkownika, jego zachowaniach, predyspozycjach i potrzebach można zminimalizować niebezpieczne zachowania pracowników.

Jednym z kluczowych problemów, z jakimi borykają się użytkownicy, producenci oraz właściciele sieci, jak również specjaliści ds. cyberbezpieczeństwa, w tym członkowie zespołów CSIRT (*Computer Security Incident Response Team*), jest identyfikacja podatności aplikacji, systemów i urządzeń, w szczególności urządzeń Internetu Rzeczy (ang. *Internet of Things, IoT*). Większość podatności jest znana przede wszystkim specjalistom ds. cyberbezpieczeństwa, natomiast często nie są one publicznie dostępne i znane użytkownikom urządzeń, co sprawia, że użytkownicy są najbardziej narażeni na zagrożenia. Dlatego rozwijanie kompetencji cyfrowych, w tym świadomości w zakresie cyberbezpieczeństwa, w różnych grupach społecznych ma kluczowe znaczenie dla zapewnienia bezpiecznego i odpornego społeczeństwa cyfrowego. Oto kilka kluczowych punktów dotyczących znaczenia szerzenia świadomości w zakresie cyberbezpieczeństwa:

- Ochrona osób i społeczności – zagrożenia cyberbezpieczeństwa, takie jak phishing, złośliwe oprogramowanie i kradzież tożsamości, mogą mieć poważne konsekwencje dla osób fizycznych, takie jak straty finansowe, naruszenia danych i prywatności. Podnoszenie świadomości na temat tych zagrożeń i promowanie najlepszych praktyk w zakresie bezpieczeństwa online może pomóc chronić ludzi przed padnięciem ofiarą cyberataków.
- Ochrona infrastruktury krytycznej – wiele systemów infrastruktury krytycznej, takich jak sieci energetyczne, sieci transportowe i placówki opieki zdrowotnej, w dużym stopniu opiera się na technologiach cyfrowych. Cyberatak na te systemy może mieć katastrofalny wpływ na bezpieczeństwo publiczne i narodowe. Zwiększanie świadomości w zakresie cyberbezpieczeństwa wśród pracowników i interesariuszy zaangażowanych w zarządzanie tymi systemami ma zasadnicze znaczenie dla ograniczania ryzyka.
- Wspieranie zaufania do usług cyfrowych – w miarę jak coraz więcej usług i transakcji przenosi się do Internetu, zapewnienie bezpieczeństwa i prywatności platform cyfrowych ma kluczowe znaczenie dla utrzymania zaufania publicznego. Edukacja użytkowników w zakresie bezpiecznych praktyk online, takich jak silne zarządzanie hasłami i rozpoznawanie podejrzanych działań, może pomóc w budowaniu zaufania do usług cyfrowych.
- Wzmocnienie pozycji wrażliwych grup – niektóre grupy społeczne, takie jak osoby starsze, dzieci i osoby o ograniczonych umiejętnościach cyfrowych, mogą być bardziej podatne na zagrożenia cybernetyczne z powodu braku świadomości lub wiedzy technicznej. Ukierunkowane programy edukacyjne w zakresie cyberbezpieczeństwa mogą umożliwić tym grupom bezpieczne i pewne poruszanie się po cyfrowym świecie.

Promowanie odpowiedzialnego obywatelstwa cyfrowego – w coraz bardziej połączonym świecie indywidualne działania w sferze cyfrowej mogą mieć daleko idące konsekwencje. Podnoszenie świadomości w zakresie cyberbezpieczeństwa sprzyja poczuciu odpowiedzialnego obywatelstwa cyfrowego, w którym jednostki rozumieją swoją rolę w ochronie siebie i innych przed zagrożeniami cybernetycznymi.

Rozwiązanie problemu luki w umiejętnościach w zakresie cyberbezpieczeństwa – ponieważ zapotrzebowanie na specjalistów ds. cyberbezpieczeństwa stale rośnie, promowanie edukacji i świadomości w zakresie cyberbezpieczeństwa od najmłodszych lat może pomóc w rozwijaniu talentów i wyeliminowaniu luki w umiejętnościach w tej dziedzinie.

Aby skutecznie szerzyć świadomość w zakresie cyberbezpieczeństwa, konieczne jest podejście obejmujące wiele zainteresowanych stron, w tym rządy, instytucje edukacyjne, przedsiębiorstwa i organizacje społeczeństwa obywatelskiego. Inicjatywy takie jak publiczne kampanie uświadamiające, programy nauczania cyberbezpieczeństwa w szkołach i na uniwersytetach oraz programy szkoleniowe dla pracowników mogą przyczynić się do budowania społeczeństwa bardziej odpornego na zagrożenia cybernetyczne.

Podnoszenie świadomości użytkowników na temat zagrożeń związanych z posiadaniem i korzystaniem z niezabezpieczonych urządzeń oraz zapewnienie dostępu do informacji na temat luk w zabezpieczeniach jest kluczowe. Opracowane w NASK-PIB centralne repozytorium informacji o lukach w zabezpieczeniach i exploitach związanych z urządzeniami IoT [31] odpowiada na tę potrzebę. Więcej informacji na temat sposobu kolekcjonowania danych oraz budowania bazy można znaleźć w pracach [32, 33], natomiast możliwości wykorzystania serwisu zostały szerzej opisane w publikacji [34].

## PODSUMOWANIE

Wdrożenie solidnych środków cyberbezpieczeństwa może być finansowo obciążające, zwłaszcza dla mniejszych organizacji, gdyż wymaga znacznych inwestycji w technologie, personel i utrzymanie systemów. Popyt na wykwalifikowanych specjalistów ds. cyberbezpieczeństwa przewyższa podaż, co utrudnia organizacjom znalezienie i utrzymanie ekspertów niezbędnych do skutecznego zarządzania bezpieczeństwem.

Szybka ewolucja technologii może prowadzić do wysoce złożonego krajobrazu, wprowadzając potencjalnie nowe luki w zabezpieczeniach z powodu błędnej konfiguracji, diagnostyki lub niewystarczającego zrozumienia systemów. Dlatego kluczowe jest ciągłe doskonalenie strategii ochrony oraz inwestowanie w edukację i rozwój specjalistów w tej dziedzinie.

Do kluczowych kierunków przyszłych badań należy zatem zaliczyć:

- Opracowanie lekkich i wydajnych modeli sztucznej inteligencji (AI) i uczenia maszynowego (ML), w szczególności dla urządzeń Internetu Rzeczy (IoT) o ograniczonych zasobach, przy jednoczesnym zapewnieniu bezpieczeństwa i prywatności. Wykorzystanie AI/ML do wykrywania zagrożeń, analizy behawioralnej, analizy predykcyjnej oraz przetwarzania języka naturalnego do identyfikacji phishingu i złośliwych treści, a także uwierzytelniania adaptacyjnego. Badanie technik AI/ML w celu wykrywania podatności typu zero-day poprzez analizę kodu i zachowania systemu.
- Integrację technologii blockchain w celu bezpiecznego i przejrzystego udostępniania danych oraz zarządzania informacją pomiędzy interesariuszami, komputerami, urządzeniami i czujnikami. Opracowanie nowych mechanizmów uwierzytelniania opartych na lekkim szyfrowaniu kwantowym. Badanie zdecentralizowanych, zorientowanych na użytkownika i kontekstowych modeli kontroli dostępu.
- Adresowanie kwestii prywatności i etyki w gromadzeniu, przetwarzaniu i udostępnianiu danych, szczególnie w środowisku wszechobecnych komputerów oraz technologii IoT.
- Opracowanie nowych modeli bezpieczeństwa i protokołów zabezpieczających komunikację oraz wymianę danych pomiędzy heterogenicznymi urządzeniami i sieciami IoT. Przyjęcie wszechobecnych rozwiązań bezpieczeństwa opartych na sprzęcie, takich jak zaufane środowiska wykonawcze, bezpieczny rozruch i bezpieczne przechowywanie, w celu zapobiegania fizycznym manipulacjom i atakom.
- Zdefiniowanie rygorystycznych specyfikacji bezpieczeństwa jako podstawy do opracowania bezpiecznych urządzeń, chipsetów i sieci IoT, obejmujących interdyscyplinarną współpracę między zainteresowanymi stronami. Ulepszenie modeli w obszarze cyberbezpieczeństwa dla świadomości sytuacyjnej na wszystkich poziomach w celu uniknięcia sprzecznych interesów i priorytetów.

Kierunki te obejmują szeroki zakres obszarów, w tym integrację AI/ML, nowe technologie, takie jak blockchain i szyfrowanie kwantowe, prywatność i kwestie etyczne, nowe protokoły i modele bezpieczeństwa oraz holistyczne ramy i strategię cyberbezpieczeństwa dostosowaną do ekosystemu wszechobecnego internetu oraz rozbudowanej sieci sensorów.

Chociaż nowoczesne technologie poprawiają cyberochronę dzięki zaawansowanym narzędziom i technikom, wprowadzają również nowe wyzwania i zagrożenia. Osiągnięcie równowagi między solidnymi środkami bezpieczeństwa a zachowaniem prawa do prywatności, przy jednoczesnym sprostaniu wyzwaniom ekonomicznym i związanym z niedoborem wykwalifikowanych specjalistów, jest niezbędne dla pełnego wykorzystania postępu technologicznego w dziedzinie cyberbezpieczeństwa. Tylko takie podejście pozwoli na maksymalizację korzyści wynikających z nowoczesnych rozwiązań technologicznych, przy jednoczesnym minimalizowaniu ryzyka i ochronie praw jednostek.

Należy również zaznaczyć, że zasadniczą rolę w zapewnianiu stabilności i ciągłości funkcjonowania kraju, gospodarki i społeczeństwa odgrywa infrastruktura krytyczna, obejmująca m.in. sieci energetyczne, systemy transportowe i placówki opieki zdrowotnej. W odpowiedzi na szybko zmieniające się warunki w zakresie bezpieczeństwa narodowego i międzynarodowego, w aktualizacji Narodowego Programu Ochrony Infrastruktury Krytycznej z 2023 roku wskazano na szereg nowych wyzwań i zaakcentowano potrzebę adaptacji strategii ochrony infrastruktury krytycznej, w tym sieci internetowej, do zmieniających się zagrożeń technologicznych i geopolitycznych [35].

Dodatkowo, dyrektywa NIS2 (Network and Information Systems Directive 2) z 2022 r. wprowadziła nowe wymagania dotyczące ochrony infrastruktury krytycznej w kontekście cyberbezpieczeństwa [36]. Dyrektywa ta zobowiązuje państwa członkowskie Unii Europejskiej do wdrożenia bardziej rygorystycznych środków ochrony i monitorowania infrastruktury krytycznej, w celu zwiększenia odporności na cyberataki oraz zapewnienia stabilności operacyjnej. Wprowadzenie NIS2 ma na celu zwiększenie poziomu zabezpieczeń oraz harmonizację standardów bezpieczeństwa w całej Unii Europejskiej, co jest kluczowe w kontekście współczesnych, transgranicznych zagrożeń cybernetycznych. Adaptacja tych regulacji jest konieczna dla skutecznego zarządzania ryzykiem i minimalizacji potencjalnych skutków incydentów cybernetycznych na funkcjonowanie kluczowych sektorów gospodarki i życia społecznego.

W kontekście tych wszystkich wyzwań, coraz większe znaczenie zyskują technologie i zabezpieczenia postkwantowe. Rozwój komputerów kwantowych stawia nowe wyzwania przed tradycyjnymi metodami kryptograficznymi, które mogą stać się podatne na ataki przy użyciu technologii kwantowych. W związku z tym, badania nad postkwantowymi algorytmami szyfrowania, takimi jak kryptografia oparta na kratach (ang. *lattice-based cryptography*), stają się priorytetem, a implementacja tych zaawansowanych technologii zabezpieczeń jest niezbędna do zapewnienia długoterminowej ochrony infrastruktury przed przyszłymi zagrożeniami.

## BIBLIOGRAFIA


[1] Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/

[2] Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. Technology Innovation Management Review, 4(10), 13–21. http://timreview.ca/article/835

[3] NASK. (2024, lipiec 5). NASK ostrzega: rośnie liczba oszustw deepfake wykorzystujących wizerunki znanych osób. Pobrane z https://www.nask.pl/pl/aktualnosci/5403,NASK-ostrzega-rosnie-liczba-oszustw-deepfake-wykorzystujacych-wizerunki-znanych-.html

[4] Ibrahim, A., Thiruvady, D., Schneider, J.-G., & Abdelrazek, M. (2020). The challenges of leveraging threat intelligence to stop data breaches. Frontiers in Computer Science, 2, 36. https://doi.org/10.3389/fcomp.2020.00036

[5] Grzenda, M., Kaźmierczak, S., Luckner, M., Borowik, G., & Mańdziuk, J. (2023). Evaluation of machine learning methods for impostor detection in web applications. Expert Systems With Applications, 231(2023), 120736. https://doi.org/10.1016/j.eswa.2023.120736

[6] Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. Technology Innovation Management Review, 9(11), 39-52.

[7] Alanazi, S., Asif, S & Moulitsas, I. (2024). Examining the Societal Impact and Legislative Requirements of Deepfake Technology: A Comprehensive Study. International Journal of Social Science and Humanity, 14(2), 58-64.

[8] Bray, S.D., Johnson, S.D., Kleinberg, B. (2023). Testing human ability to detect 'deepfake' images of human faces. Journal of Cybersecurity, 9(1), 1-18.

[9] Rana, M.S., Nobi, M.N., Murali, B. & Sung, A.H. (2022). Deepfake Detection: A Systematic Literature Review. IEEE Access, 10, 25494-25513.

[10] Zhang, T. (2022). Deepfake generation and detection, a survey. Multimedia Tools and Applications, 81, 6259–6276.

[11] Cloudflare DDoS Protection Team. (2024). DDoS Attack Trends for 2023 Q4. Dostęp zdalny (20.02.2024): https://radar.cloudflare.com/reports/ddos-2023-q4

[12] Pilkington, M. (2016). Blockchain technology: principles and applications. W: F. X. Olleros & M. Zhegu (Reds.), Research Handbook on Digital Transformations. Edward Elgar Publishing, Cheltenham, UK, Northampton, USA.

[13] Swan, M. (2015). Blockchain: Blueprint for a new economy. O'Reilly Media, Inc.

[14] Wright, A., & De Filippi, P. (2015). Decentralized blockchain technology and the rise of lex cryptographia. Pobrano 27 grudnia 2018, z https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

[15] Mendling, J., Weber, I., van der Aalst, W., van den Brocke, J., Cabanillas, C., Daniel, F., & Gal, A. (2018). Blockchains for business process management – Challenges and opportunities. ACM Transactions on Management Information Systems (TMIS), 9(1).

[16] Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the bitcoin ecosystem. IEEE APWG eCrime Researchers Summit.

[17] Chapron, G. (2017). The environment needs cryptogovernance. Nature, 545, 403–405.

[18] Brown, S. D. (2016). Cryptocurrency and criminality: The Bitcoin opportunity. The Police Journal, 89(4), 327–339.

[19] Tziakouris, G. (2018). Cryptocurrencies – A forensic challenge or opportunity for law enforcement? An INTERPOL perspective. IEEE Security & Privacy, 16(4), 92–94.

[20] Borowik, G., Wawrzyniak, Z., & Cichosz, P. (2019). Technologia blockchain — innowacja i bezpieczeństwo. Przegląd Policyjny, 136(4), 40-59.

[21] Radford, A., Wu, J., Child, R., Luan, D., Amodei, D., & Sutskever, I. (2019). Language models are unsupervised multitask learners. OpenAI Blog.

[22] ENISA. (2023). Cybersecurity of AI and Standardisation. Retrieved January 22, 2024, from https://www.enisa.europa.eu/publications/cybersecurity-of-ai-and-standardisation

[23] ISO/IEC 38507:2022. Information technology - Governance of IT - Governance implications of the use of artificial intelligence by organizations. ISO.

[24] ISO/IEC 27001:2022. Information security management systems - Requirements. ISO.

[25] Duta, K. A. (2021). Detecting phishing websites using machine learning technique. PloS one. https://doi.org/10.1371/journal.pone.0258361

[26] Mittal, M., Kumar, K., & Behal, S. (2022). Deep learning approaches for detecting DDoS attacks: a systematic review. Soft Computing. https://doi.org/10.1007/s00500-021-06608-1

[27] Kim, B., Xiong, A., Lee, D., & Han, K. (2021). A systematic review on fake news research through the lens of news creation and consumption: Research efforts, challenges, and future directions. PLOS ONE. https://doi.org/10.1371/journal.pone.0277111

[28] Xu, Z., Li, J., Pan, Y., Lazos, L., Li, M., & Ghose, N. (2023). Proof-of-Following for Vehicle Platoons. arXiv preprint arXiv:2107.09863v4.

[29] Richardson, J., Samara, V., Styslavska, O., & Manders, T. (2022, October). Closing the gap between the needs of the cybersecurity industry and the skills of tertiary education graduates. ISC3C. https://is3coalition.org/docs/study-report-is3c-cybersecurity-skills-gap/

[30] PeopleKeys, https://peoplekeys.com/ (dostęp 17.06.2024)

[31] VARIoT baza podatności i eksploitów IoT, https://www.variotdbs.pl/

[32] Rytel, M., Felkner, A., & Janiszewski, M. (2020). Towards a safer Internet of Things – A survey of IoT vulnerability data sources. Sensors, 20(21).

[33] Janiszewski, M., Felkner, A., Lewandowski, P., Rytel, M., & Romanowski, H. (2021). Automatic actionable information processing and trust management towards safer Internet of Things. Sensors, 21(13).

[34] Felkner, A. (2023). Źródła użytecznych informacji o zagrożeniach w internecie rzeczy. Cybersecurity and Law, 9(1), 144-154.

[35] Rządowe Centrum Bezpieczeństwa. (2023). Narodowy Program Ochrony Infrastruktury Krytycznej. Rządowe Centrum Bezpieczeństwa. Pobrano z https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej

[36] Parlament Europejski i Rada UE. (2022). Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii. Pobrane z https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32022L2555

[37] Post-Quantum Cryptography Initiative, https://www.cisa.gov/quantum (dostęp 17.06.2024)

DOI: 10.15199/59.2024.4.2

# Zastosowanie metod uczenia maszynowego w sieciach teleinformatycznych

## Application of machine learning methods in communication networks

Prof. dr hab. inż. KRZYSZTOF WALKOWIAK[1],
mgr inż. ALEKSANDRA KNAPIŃSKA[1], dr inż. PIOTR LECHOWICZ[1,2]

[1] Politechnika Wrocławska, Wrocław
email: krzysztof.walkowiak@pwr.edu.pl
[2] Chalmers University of Technology, Gothenburg, Sweden

STRESZCZENIE W ostatnich latach ważnym czynnikiem wpływającym na rozwój sieci teleinformatycznych są metody uczenia maszynowego. Wynika to głównie z dużej konkurencji na rynku usług sieciowych, co pociąga za sobą bezustanną potrzebę jednoczesnego usprawnienia działania sieci komputerowych oraz obniżania kosztów działania sieci komputerowych. W artykule zostaną omówione przykładowe zastosowania metod uczenia maszynowego w sieciach teleinformatycznych. Zostaną przedstawione najnowsze technologie sieci teleinformatycznych, w których stosowane są metody uczenia maszynowego, w tym: automatyzacja sieci oraz koncepcja cyfrowego bliźniaka. Zostaną również zaprezentowane najważniejsze wyzwania związane ze stosowaniem metod uczenia maszynowego w sieciach teleinformatycznych, takie jak: dostęp do danych, potrzeba ciągłej aktualizacji modeli w związku ze zmieniającymi się wzorcami w sieciach, wyjaśnialną sztuczną inteligencję (ang. Explainable Artificial Intelligence).
SŁOWA KLUCZOWE sieci teleinformatyczne, uczenie maszynowe, optymalizacja, automatyzacja sieci, cyfrowy bliźniak

ABSTRACT In recent years, machine learning (ML) methods have been an important factor influencing the development of communications networks. This is mainly due to the high competition in the ICT sector, which entails a relentless need to simultaneously improve the operation of communication computer and reduce the OPEX and CAPEX cost of networks. The paper will discuss examples of applications of machine learning methods in communication networks. The latest networking technologies that use machine learning methods will be presented, including network automation and digital twin. The most important challenges of applying machine learning methods in communication networks will also be described, including: datasets, updating ML models to changing patterns in networks, Explainable Artificial Intelligence.
Keywords: communication network, machine learning, optimization, network automation, digital twin
KEYWORDS: Microstrip antennas, antenna simulation, antenna gain, reflection coefficient, FDTD method, multi-system antennas

Od wielu lat jednym z głównych powodów prowadzenia badań naukowych w obszarze sieci teleinformatycznych jest nieustanny wzrost ruchu w sieci Internet. Jednak w ostatnim okresie dynamika tego wzrostu spada. W raporcie Ericsson Mobility Report opublikowanym w czerwcu 2024 r. dynamika rocznego wzrostu ruchu w sieciach mobilnych spadła w pierwszym kwartale 2024 r. do 25%, podczas gdy w 2018 r. roczny wzrost ruchu wynosił ponad 95% [1]. Innym ważnym czynnikiem wpływającym na badania naukowe w obszarze sieci teleinformatycznych są aspekty ekonomiczne związane z bardzo dużą konkurencją na rynku usług sieciowych. W celu obniżenia kosztów działania i zwiększenia zysku, operatorzy sieciowi w coraz większym stopniu wprowadzają rozwiązania wykorzystujące metody uczenia maszynowego związane z automatyzacją sieci (ang. *network automation*), co przede wszystkim umożliwia zmniejszenie zatrudnienia [2] i poprawienia jakości oferowanych usług. Ponadto jako powody stosowania metod uczenia maszynowego w sieciach teleinformatycznych należy także wymienić: wysoki stopień złożoności systemów sieciowych oraz szybko rosnącą ilość danych gromadzonych w sieciach teleinformatycznych [3].

Dwa najważniejsze rodzaje metody uczenia maszynowego stosowane w sieciach teleinformatycznych obejmują [3, 4]:

- Uczenie nadzorowane (ang. *supervised learning*) – algorytm jest trenowany na podstawie odpowiednio opisanych danych wzorcowych zawierających rozwiązanie problemu, tzw. etykiety albo klasy. Dzięki temu algorytm uczy się rozpoznawać cechy obiektów zapisane w danych trenujących, co umożliwia prawidłowe klasyfikowanie nowych danych, które pojawią się w przyszłości. W ramach metod uczenia nadzorowanego rozróżniamy dwie grupy metod rozwiązujące: problem regresji, w którym przewidywane są wartości i problem klasyfikacji,

w którym przewidywane są klasy. Jako przykład regresji można wskazać prognozowanie poziomu wolumenu ruchu sieciowego w przyszłości na podstawie danych historycznych. Przykładem klasyfikacji może być zakwalifikowania pakietów sieciowych do określonego rodzaju usługi sieciowej.

- Uczenie nienadzorowane (ang. *unsupervised learning*) – algorytm jest trenowany na podstawie danych, które są nieoznakowane tzn. nie posiadają etykiet albo klas. Metody uczenia nienadzorowanego umożliwiają poznanie wzorców i struktur w analizowanych obiektach, np. segmentowanie danych w grupy według cech zapisanych w danych oraz detekcję anomalii poprzez rozpoznanie wzorca odbiegającego od reszty danych. Do metod uczenia nienadzorowanego należą m.in. algorytmy analizy skupień (ang. *clustering*) nazywane także algorytmami klasteryzacji albo grupowania.

Więcej informacji na temat metod uczenia maszynowego w kontekście zastosowań w sieciach teleinformatycznych można znaleźć w pracach [3–8].

Głównym celem tego artykułu jest przedstawienie przykładów zastosowań metod uczenia maszynowego w sieciach teleinformatycznych. W szczególności, zostaną omówione najnowsze koncepcje pojawiające się w badaniach naukowych w obszarze sieci teleinformatycznych, w których wykorzystywane są metody uczenia maszynowego, w tym: automatyzacja sieci oraz koncepcja cyfrowego bliźniaka. Ponadto, zostaną przedstawione istotne problemy związane ze stosowaniem metod uczenia maszynowego w sieciach teleinformatycznych: dostęp do danych, potrzeba ciągłej aktualizacji modeli w związku ze zmieniającymi się wzorcami w sieciach, wyjaśnialna sztuczna inteligencja (ang. *Explainable Artificial Intelligence*).

Artykuł przedstawia najnowsze trendy obserwowane obecnie w sieciach teleinformatycznych oraz omawia przykłady zastosowań metod uczenia maszynowego w sieciach teleinformatycznych.

## NAJNOWSZE TRENDY W SIECIACH TELEINFORMATYCZNYCH

### Automatyzacja sieci

Rosnąca złożoność sieci teleinformatycznych stanowi wyzwanie dla zapewnienia użytkownikom wysokiej jakości usług. Automatyzacja sieci (ang. *network automation*) to proces automatyzacji konfigurowania, zarządzania, testowania, wdrażania i obsługi urządzeń fizycznych i wirtualnych w sieciach teleinformatycznych. Głównymi celami automatyzacji jest obniżenie kosztów zarządzania siecią oraz poprawienie jakości działania sieci. Najważniejszymi technologiami umożliwiającymi automatyzację sieci bez konieczności ingerencji człowieka w jej działanie (ang. *Zero Touch Management*) są programowalne sieci (ang. *Sofware Defined Networks*), wirtualizacja i orkiestracja sieci, monitorowanie parametrów, analiza danych oraz zamknięta pętla sterowania siecią [5, 9].

W pracy [5] koncepcja ZTM (Zero Touch Management) jest definiowana jako w pełni autonomiczne rozwiązanie służące do zarządzania siecią, ale stosowane z nadzorem człowieka. Technologie ZTM muszą być w stanie analizować oraz interpretować dostarczane dane i na tej podstawie proponować zalecenia związane z automatyzacją sieci w oparciu o rozwiązania sztucznej inteligencji i uczenia maszynowego. Stosowanie koncepcji ZTM jest związane z potrzebą zapewnienia jak największej elastyczności działania sieci i umiejętności adaptacji do zmieniających się warunków działania sieci oraz ewoluujących potrzeb biznesowych. Dla realizacji koncepcji ZTM w sieciach teleinformatycznych używających sprzętu wielu dostawców, oraz w sieciach wielodomenowych, ważnym elementem jest standaryzacja współpracy różnych komponentów systemów analizy danych oraz zapewnienie kontroli sieci w zamkniętej pętli (ang. *closed loop*). Pozwala to na efektywne tworzenie, wykonywanie i zarządzanie zarówno pojedynczymi, jak i bardziej złożonymi procesami, realizowanymi w formie zamkniętej pętli.

Kolejną ważną koncepcją związaną z automatyzacją sieci są sieci intuicyjne IBN (ang. *Intent-Based Networking*). Koncepcja IBN służy do zastąpienia ręcznego konfigurowania sieci poprzez zastosowanie kontrolera sieciowego, który jest w stanie przetłumaczyć intencje klientów na zasady, które można w sposób automatyczny zaimplementować w sieci. Intencja (ang. *intent*) jest rozumiana jako prosty wymóg deklaratywny, który powinien odzwierciedlać to, czego użytkownik oczekuje od sieci. Głównym celem stosowania IBN jest zapewnienie ciągłego dostosowywania działania sieci teleinformatycznych pod kątem potrzeb biznesowych [10–12].

System IBN działa w zamkniętej pętli w oparciu o następujące komponenty [10]:

- Profilowanie intencji (ang. *intent profiling*). Użytkownik wchodzi w interakcję z systemem IBN, aby wyrazić swoją intencję. W przeciwieństwie do poleceń wpisanych w linii komend lub zgłoszonych za pomocą interfejsu API (ang. *application programming interface*), intencje powinny być przekazywane w sposób przyjazny dla człowieka (np. poprzez wyrażenia w języku naturalnym, rozwijane menu itp.).
- Tłumaczenie intencji (ang. *intent translation*). Po przesłaniu intencji do systemu IBN, intencja powinna zostać przetłumaczona i przekształcona w niskopoziomowe konfiguracje sieciowe, które można zastosować do skonfigurowania urządzeń sieciowych. W celu tłumaczenia instrukcji wykorzystywane są duże modele językowe (ang. *large language model*) oraz generatywna sztuczna inteligencja (ang. *generative artificial inteligence*).
- Rozstrzyganie intencji (ang. *intent resolution*). Użytkownik może przesłać swoją intencję niezależnie od innych użytkowników lub grupy użytkowników, którzy mogą współistnieć w tym samym czasie w sieci. Może to łatwo prowadzić do sprzecznych lub konfliktowych konfiguracji sieci, które będą miały wpływ na nowe lub już zaimplementowane intencje. Dlatego system IBN powinien być

wyposażony w moduł rozwiązywania polityk sieciowych, który będzie w stanie rozwiązywać potencjalne konflikty.
- Aktywacja intencji (ang. *intent activation*). Kiedy system IBN upewni się, że aktywacja nowej intencji nie wpłynie na inne istniejące implementacje intencji, powinien zapewniać realizację żądanej usługi sieciowej. Niemniej jednak intencje to nie tylko żądania realizacji ogólnych usług sieciowych, ale mogą one również zawierać spersonalizowane oczekiwania użytkowników. W związku z tym system IBN musi implementować każdą intencję w odpowiednio dostosowany sposób, który zapewni skonfigurowanie sieci zgodnie z oczekiwaniami użytkownika.
- Realizacja intencji (ang. *intent assurance*). Komponent aktywacji intencji zapewni, że intencja będzie zaimplementowana w sieci. Ponieważ sieci teleinformatyczne nie są statyczne i mają często dynamiczny charakter, niezbędnym elementem systemu IBN jest także komponent realizacji intencji. Głównym zadaniem tego komponentu jest kontrola czy intencja jest realizowana w prawidłowy sposób przez cały okres istnienia danej intencji. W tym celu komponent realizacji intencji musi podejmować proaktywne oraz reaktywne działania w zakresie samokonfiguracji i samonaprawy sieci zgodnie z daną intencją i wspierać użytkowników pod kątem możliwości modyfikacji ich intencji, w sytuacji kiedy powstanie luka między oczekiwaniami użytkowników, a zachowaniem sieci.

Do analizy danych w technologiach automatyzacji sieci często wykorzystywane są metody uczenia maszynowego. Przykładami zastosowań są:
- Detekcja anomalii w działaniu sieci mogąca wynikać z pogarszającej się jakości urządzeń sieciowych, złej konfiguracji urządzeń [6].
- Automatyczna rekonfiguracja wirtualnej topologii [7].
- Predykcja jakości transmisji (ang. *quality of transmission*) zestawianych połączeń [8].
- Klasyfikacja słów i wyrażeń w intencjach sieciowych pod kątem dobrania odpowiednich polityk sieciowych do realizacji danej intencji [5].

### Cyfrowy bliźniak

Koncepcja cyfrowego bliźniaka (ang. *digitial twin*) jest wykorzystywana w wielu sektorach przemysłu do modelowania procesów w złożonych systemach dynamicznych. Cyfrowy bliźniak można zdefiniować jako wirtualną kopię rzeczywistego fizycznego obiektu, systemu lub zjawiska, która jest stworzona jako model w środowisku cyfrowym. Jako główne zalety cyfrowych bliźniaków należy wymienić fakt, że mogą one dokładnie modelować złożone systemy i w ten sposób mogą służyć do symulacji różnych sytuacji i procesów w tych systemach. Cyfrowe bliźniaki są stosowane przede wszystkim w kontekście: inteligentnej produkcji w celu poprawienia wydajności działania złożonych produktów inżynieryjnych (np. projektowanie silników), modelowanie interakcji fizycznych (np. systemy grawitacyjne), rozwijania koncepcji inteligentnego miasta. Głównym celem rozwijania cyfrowego bliźniaka sieci (ang. *network digitial twin*) jest wsparcie szeroko pojętego procesu zarządzania siecią. Ważnym elementem w tworzeniu cyfrowego bliźniaka sieci są metody uczenia maszynowego, które mogą być wykorzystane do modelowania działania różnych elementów sieci teleinformatycznych w sposób dokładniejszy i szybszy niż inne metody (np. symulator sieciowy, modele analityczne) [13–15].

Jako najważniejsze przykłady zastosowań koncepcji cyfrowego bliźniaka w sieciach teleinformatycznych należy wymienić [14, 15]:
- Rozwiązywanie problemów. Operatorzy sieciowi za pomocą cyfrowego bliźniaka mogą modelować rożne scenariusze zaobserwowane w przeszłości w celu znalezienia potencjalnych przyczyn zakłóceń działania sieci.
- Analiza „co jeśli" (ang. *What-if Analysis*). Cyfrowy bliźniak może być wykorzystany jako bezpieczne środowisko testowe, w którem można zastosować różne konfiguracje sieci, aby zrozumieć ich wpływ na wydajność sieci. Dzięki temu nie ma potrzeby testowania konfiguracji w sieci produkcyjnej.
- Planowanie sieci. Cyfrowy bliźniak może być wykorzystany do oszacowania, kiedy istniejąca sieć będzie wymagała aktualizacji. Jest to realizowane poprzez różnego rodzaju symulacje związanie z rozwojem sieci (np. wzrostem ruchu sieciowego) i obserwacją stanu sieci.
- Wykrywanie anomalii. W sytuacji kiedy zachowanie rzeczywistej sieci odbiega od normalnych scenariuszy operacyjnych, cyfrowy bliźniak może być wykorzystany do identyfikacji anomalii i wskazania potencjalnych przyczyny występowania anomalii.
- Konfiguracja urządzeń sieci optycznych. Cyfrowy bliźniak może być wykorzystany do określenia różnych parametrów fizycznych sieci optycznej co umożliwia dostosowanie lepszą konfiguracji urządzeń sieciowych w warstwie fizycznej zapewniającą bardziej wydajne działanie sieci i zmniejszenie prawdopodobieństwo blokowania.

## PRZYKŁADY ZASTOSOWAŃ METOD UCZENIA MASZYNOWEGO W OPTYMALIZACJI SIECI TELEINFORMATYCZNYCH

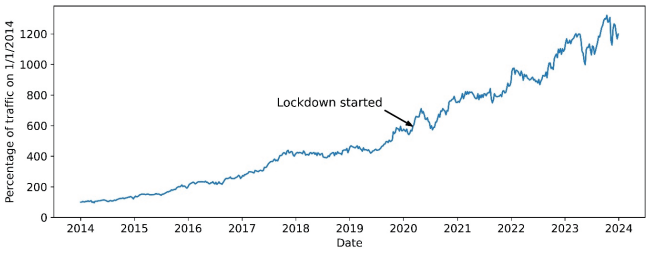
W tym rozdziale zostaną omówione przykłady zastosowania metod uczenia maszynowego w sieciach teleinformatycznych. Na początku przedstawimy zagadnienia związane z uzyskaniem danych do badań w zakresie uczenia maszynowego. Następnie, skupimy się na dwóch obszarach: predykcji ruchu sieciowego oraz koncepcji cyfrowego bliźniaka sieci.

### Dane

Bardzo ważnym elementem w stosowaniu metod uczenia maszynowego jest uzyskanie zbiorów danych dotyczących rozważanych problemów badawczych. Dane są niezbędne w procesie trenowania modeli uczenia maszynowego oraz następnie w procesie testowania opracowanych modeli uczenia maszynowego. Brak danych lub ich niewystar-

czająca ilość uniemożliwia realizację badań naukowych w zakresie uczenia maszynowego. W badaniach dotyczących stosowania uczenia maszynowego w sieciach teleinformatycznych zazwyczaj stosowane są następujące dwa rodzaje danych:

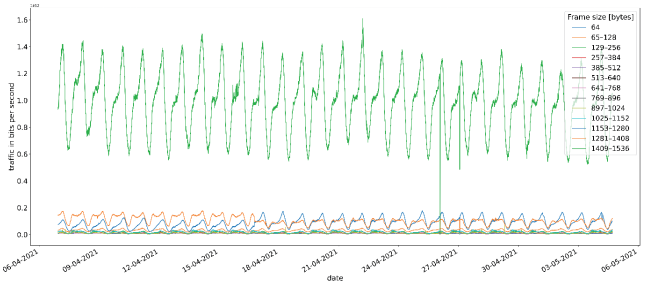
- Dane rzeczywiste uzyskane na podstawie obserwacji działających systemów sieciowych.
- Dane syntetyczne sztucznie generowane w oparciu o różne rozkłady prawdopodobieństwa lub z wykorzystaniem symulacji komputerowych. W ramach danych syntetycznych można wyróżnić dane półsyntetyczne (ang. *semi-synthetic*), które są generowane sztucznie, ale główne parametry generowanych danych są oparte na trendach obserwowanych w danych rzeczywistych




» *Rys. 1. Wzrost sumarycznego ruchu w SIX w ostatnich 10 latach – procent bitrate względem 1 stycznia 2014 [16]*
» *Fig. 1. Total traffic growth in SIX in the last 10 years – percentage bitrate compared to January 1, 2014 [16]*

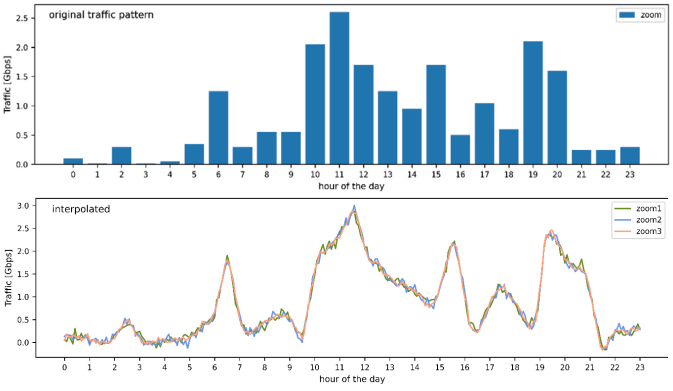
W obszarze sieci teleinformatycznych uzyskanie danych rzeczywistych jest trudne, ponieważ operatorzy sieciowi nie chcą udostępniać posiadanych danych ze względów biznesowych oraz ze względu na ochronę danych osobowych. Jednym z nielicznych miejsc, gdzie można uzyskać dane rzeczywiste o ruchu sieciowym jest punkt wymiany ruchu internetowego (ang. *Internet Exchange Point*) SIX w Seattle [16]. Do punktu wymiany ruchu internetowego SIX podłączonych jest 368 systemów autonomicznych/437 routerów. Na stronie SIX udostępnione są statystyki od roku 1997, które stanowią przydatną bazę danych o ruchu sieciowym. Udostępniane dane pokazują między innymi dynamikę wzrostu ruchu w kolejnych latach. Na *Rys. 1* przedstawiono wzrost ruchu w ostatnich 10 latach pokazany jako procent wolumenu ruchu w dniu 1.01.2014. Należy zaznaczyć, że analiza i modelowanie długoterminowych trendów wzrostu ruchu są bardzo ważnym elementem przy tworzeniu algorytmów planowania sieci i migracji do nowszych technologii [17, 18].

Oprócz sumarycznego wolumenu ruchu sieciowego, SIX publikuje również inne szczegółowe statystyki, w tym rozkład ruchu dla różnych wielkości ramek sieciowych. Ponieważ wolumen ruchu oraz poziom zaszumienia ruchu przesyłanego za pomocą różnych wielkości ramek znacząco się różnią, jest to bardzo dobre źródło danych do testowania jakości algorytmów predykcji ruchu [19–22]. Na *Rys. 2* pokazano ruch z SIX w podziale na wolumen ruchu obserwowany dla różnych wielkości ramek w okresie od 06.04.2021 do 06.05.2021. Przedstawione dane ilustrują tzw. dryfy koncepcji (nagłe zmiany wzorca) oraz brakujące obserwacje. Warto podkreślić, że opracowywane algorytmy predykcji ruchu sieciowego powinny uwzględniać sytuacje, w których następują nagłe zmiany obserwowanego ruchu oraz występowanie brakujących obserwacji.




» *Rys. 2. Ruch w Seattle w różnych wielkościach ramek. Reprezentatywny fragment z widocznymi dryfami koncepcji i obserwacjami odstającymi.*
» *Fig. 2. Seattle traffic in different frame sizes. Representative fragment with visible concept drift and outliers.*

W różnych raportach można znaleźć zagregowane informacje o ruchu sieciowym. Na przykład raport firmy Sandvine z 2021 r. pt. „The mobile internet phenomena report" [23] pokazuje wolumen ruch sieciowego różnych usług w podziale na poszczególne godziny doby (*Rys. 3*, góra). Tak pozyskana ilość informacji jest niewystarczająca do wytrenowania modeli uczenia maszynowego i może skutkować ich przetrenowaniem. Przetrenowany model daje świetne rezultaty na zbiorze trenującym, ale cechuje się bardzo niską dokładnością na innych danych. W celu poprawy jakości tworzonych modeli, można zastosować augmentację danych poprzez stworzenie nowych przykładów na podstawie już posiadanych informacji. Jako przykładowe rozwiązanie możliwe jest stworzenie półsyntetycznego ruchu zmiennego w czasie na podstawie podanego wzorca ruchu.

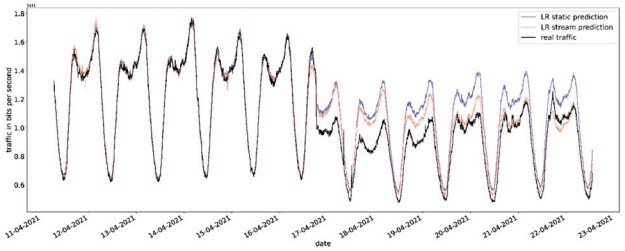



» *Rys. 3. Przykład wzorca ruchu z Raportu Sandvine [23] (na górze) oraz trzech przebiegów ruchu półsyntetycznego stworzonego za pomocą Traffic Weaver [24] (na dole)*
» *Fig. 3. Example of a traffic pattern from the Sandvine Report [23] (top) and three semi-synthetic traffic traces created with Traffic Weaver [24] (bottom)*

Wygenerowane zbiory posiadają sztucznie zwielokrotnioną liczbę obserwacji w danym oknie czasowym, zachowując zbliżoną wartość średnią sygnału. Wielokrotne odtwo-

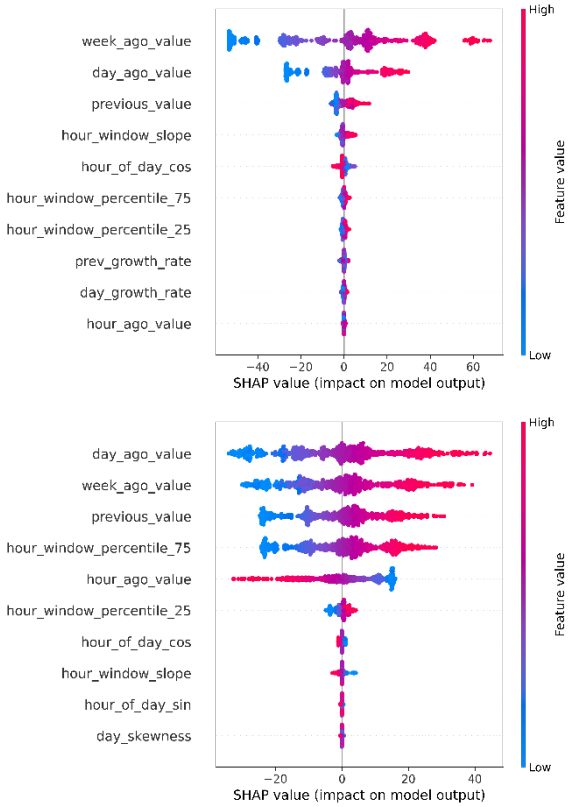
rzenia sygnału z różnymi parametrami oraz wprowadzenie dodatkowego szumu umożliwia zwielokrotnienie potrzebnych danych na potrzeby zgeneralizowania modelu uczenia maszynowego i uniknięcia przetrenowania. Narzędziem umożliwiającym ten proces jest Traffic Weaver [24], który zawiera zbiór wzorców ruchu różnych aplikacji z raportu Sandvine [23] oraz szereg narzędzi umożliwiających tworzenie danych półsyntetycznych. Możliwe jest generowanie zbiorów danych o zadanym poziomie zaszumienia, powtarzalności czy trendzie. Przykładowy źródłowy wzorzec oraz 3 półsyntetyczne przebiegi stworzone na jego podstawie zostały pokazane na rys. 3.

Predykcja ruchu sieciowegoPredykcja ruchu sieciowego ma na celu prognozowanie jego przyszłego przebiegu na podstawie danych historycznych. W literaturze został zaproponowany szereg zaawansowanych metod bazujących na analizie statystycznej oraz modelach uczenia maszynowego [25, 26]. Rzadko brane są jednak pod uwagę aspekty praktyczne, takie jak zapewnienie prognoz wysokiej jakości przez długi okres. Algorytmy są zazwyczaj testowane na małej porcji przygotowanych wcześniej danych, a ich długoterminowe działanie nie jest sprawdzane. Jak jednak można zauważyć analizując dane rzeczywiste z długich okresów, w ruchu sieciowym występują powolne trendy oraz nagłe i niespodziewane zmiany. W takich przypadkach dobrym rozwiązaniem są metody predykcji bazujące na strumieniach danych (ang. *data stream*) [20]. Takie metody ciągle dostosowują się do nowo napływających obserwacji, jednocześnie zachowując wiedzę z przeszłości. Przykład działania takich metod dostosowujących się do zmian ruchu pokazano na rys. 4. Algorytmy bazujące na strumieniach danych nadają się również do jeszcze trudniejszych przypadków, takich jak predykcja ruchu drastycznie zmieniającego się po wystąpieniu awarii i w sieci i przeprowadzeniu procesu odtworzenia ruchu (ang. *restoration*) [27].




» *Rys. 4. Predykcja ruchu sieciowego testowana na danych rzeczywistych zawierających dryfy koncepcji – adaptacja metody bazującej na strumieniach danych w porównaniu z tradycyjnym modelem trenowanym statycznie [20]*
» *Fig. 4. Network traffic prediction tested on real data containing concept drifts – adaptation of the data stream-based method compared to the traditional statically trained model [20]*

Proponowane w literaturze modele uczenia maszynowego są zazwyczaj wybierane na podstawie osiąganych wyników. Nie jest jednak analizowane ich działanie, sposób podejmowania przez nich decyzji i powiązanie cech wejściowych z prognozą. W ostatnim czasie rozwijane są jednak narzędzia wyjaśnialnej sztucznej inteligencji, które pomagają w takich analizach. Jedną z popularnych metod jest SHAP (ang. *SHapley Additive exPlanations*) [27], gdzie liczony jest wkład cech wejściowych w końcową decyzję modelu. Narzędzia wyjaśnialnej sztucznej inteligencji pozwalają usprawnić działanie modeli predykcji ruchu poprzez identyfikację głównych czynników decyzyjnych oraz cech wejściowych które nie wnoszą znaczących informacji. Taka analiza dla problemu predykcji ruchu sieciowego została przeprowadzona w pracy [29], gdzie zbadano ważność cech w zależności od stopnia zaszumienia oraz agregacji danych o ruchu sieciowym. Wzięto pod uwagę szeroki zestaw cech proponowanych w literaturze [30]. Pokazano, że modele predykcji ruchu podejmują decyzje głównie na informacjach o skorelowanych przeszłych obserwacjach, a pozostałe cechy nie wnoszą zbyt wiele informacji i nie są konieczne. Przykładowe wyniki analizy zostały pokazane na rys. 5. Przeprowadzona selekcja cech na podstawie analizy SHAP pozwoliła znacząco przyśpieszyć działanie modeli bez strat jakości predykcji.



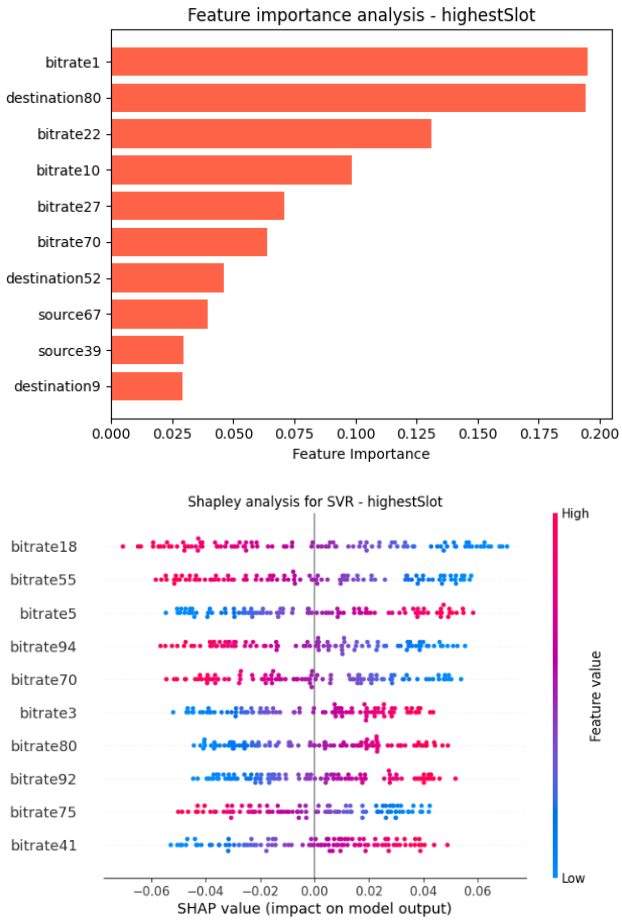

» *Rys. 5. Przykładowe wykresy analizy działania modeli predykcji ruchu sieciowego z różnymi regresorami; wkład cech w decyzję modelu policzony przy pomocy SHAP [29]*
» ***Fig. 5. Example graphs of the analysis of the performance of network traffic prediction models with different regressors; the contribution of features to the model decision calculated using SHAP [29]***

## CYFROWY BLIŹNIAK SIECI

Ocena działania algorytmów optymalizacji sieci wymaga wielu czasochłonnych i skomplikowanych symulacji. Działanie proponowanych algorytmów powinno być przetestowane z różnorodnym ruchem, aby dokładnie spraw-

dzić działanie danej metody. Jest to długotrwały proces, który wymaga dedykowanych systemów symulacji sieci lub cyfrowych bliźniaków sieci. Można jednak go przyśpieszyć, używając wyników przeprowadzonych symulacji do stworzenia modelu regresji odzwierciadlającego działanie sieci. Taki model, na podstawie macierzy ruchu sieciowego przewiduje wartość wybranych metryk działania sieci, np. użycie spektrum optycznego lub liczbę używanych transponderów.

Niedawna analiza opisana w pracy [31] pokazała, że jest możliwe stworzenie modelu, który skutecznie przewiduje różne metryki działania sieci. Co więcej, do prognozowania metryk z dobrą jakością wystarczyły dane zebrane ze 100 wcześniej przeprowadzonych symulacji. Kolejna praca [32], na podstawie analizy XAI, pokazała jak można dalej usprawnić działanie modeli regresji sieci poprzez selekcję cech. Przykładowe wyniki analizy zostały przedstawione na rys. 6. Wybierając najbardziej znaczące cechy (informacje o ruchu sieciowym) można, bez utraty jakości, pięciokrotnie przyśpieszyć czas trenowanie modelu i o 15% zmniejszyć czas predykcji.




» *Rys. 6. Przykładowe wykresy analizy działania modelu regresji sieci [32]. Ważność cech w drzewie decyzyjnym (po lewej) oraz wkład cech w decyzję modelu policzony przy pomocy SHAP (po prawej)*

» *Fig. 6. Example of graphs of the analysis of the performance of the network regression model [32]. The importance of features in the decision tree (left) and the contribution of features to the model decision calculated using SHAP (right).*

## PODSUMOWANIE

W artykule przedstawiono zagadnienia i wyzwania związane z zastosowaniem metod uczenia maszynowego w sieciach teleinformatycznych. Ze względu na rosnącą konkurencję i potrzeby optymalizacji kosztów w sektorze teleinformatycznym, stosowanie metod uczenia maszynowego odgrywa obecnie istotną rolę w wielu procesach, w tym w zakresie automatyzacji sieci oraz w koncepcji cyfrowego bliźniaka sieci. Dla dalszego rozwoju badań naukowych w obszarze stosowania metod uczenia maszynowego w sieciach teleinformatycznych ważne jest uzyskanie dostępu do zbiorów danych niezbędnych do rozwoju modeli uczenia maszynowego, a także uwzględnienie metod XAI związanych z ideą wyjaśnialności sztucznej inteligencji.

*Opracowanie artykułu zostało wsparte przez Narodowe Centrum Nauki (NCN) w ramach projektu 2019/35/B/ST7/04272*

## LITERATURA


[1] Ericsson Company, Ericsson mobility report, June 2024, https://www.ericsson.com/en/reports-and-papers/mobility-report/reports/june-2024, 2024.

[2] I. Morris, 2023 in review: Job changes and layoffs, https://www.lightreading.com/ai-machine-learning/2023-in-review-job-changes-and-layoffs, 2023.

[3] F. Musumeci, C. Rottondi, A. Nag, I. Macaluso, D. Zibar, M. Ruffini, M. Tornatore, An overview on application of machine learning techniques in optical networks, IEEE Communications Surveys & Tutorials 21 (2), 1383–1408. doi:10.1109/COMST.2018.2880039, 2018.

[4] T. Panayiotou, M. Michalopoulou, G. Ellinas, Survey on machine learning for traffic-driven service provisioning in optical networks, IEEE Communications Surveys & Tutorials 25 (2) 1412–1443. doi:10.1109/COMST.2023.3247842, 2023.

[5] E. Coronado, R. Behravesh, T. Subramanya, A. Fernàndez-Fernàndez, M. S. Siddiqui, X. Costa-Pérez, R. Riggio, Zero touch management: A survey of network automation solutions for 5g and 6g networks, IEEE Communications Surveys & Tutorials 24 (4), 2535–2578. doi:10.1109/COMST.2022.3212586, 2022.

[6] C. Natalino, A. Panahi, N. Mohammadiha, P. Monti, AI/ML-as-a-service for optical network automation: use cases and challenges [invited], Journal of Optical Communications and Networking 16 (2), A169–A179. doi:10.1364/JOCN.500706, 2024.

[7] D. Rafique, L. Velasco, Machine learning for network automation: overview, architecture, and applications [invited tutorial], Journal of Optical Communications and Networking 10 (10), D126–D143. doi:10.1364/JOCN.10.00D126, 2018.

[8] L. Zhang, X. Li, Y. Tang, J. Xin, S. Huang, A survey on QoT prediction using machine learning in optical networks, Optical Fiber Technology 68, 102804. doi:10.1016/j.yofte.2021.102804, 2022.

[9] Cisco Company, What is network automation?, https://www.cisco.com/c/en/us/solutions/automation/network-automation.html.

[10] A. Leivadeas, M. Falkner, A survey on intent-based networking, IEEE Communications Surveys Tutorials 25 (1), 625–655. doi:10.1109/COMST.2022.3215919, 2023.
[11] Cisco Company, What is intent-based networking(IBN)? https://www.cisco.com/c/en/us/solutions/intent-based-networking.html.
[12] Clemm, A., Ciavaglia, L., Granville, L., and J. Tantsura, "Intent-Based Networking – Concepts and Definitions", RFC 9315, DOI 10.17487/RFC9315, https://www.rfc-editor.org/info/rfc9315, 2022.
[13] F. Tao, H. Zhang, A. Liu, A. Y. C. Nee, Digital twin in industry: State-of-the-art, IEEE Transactions on Industrial Informatics 15 (4), 2405–2415. doi:10.1109/TII.2018.2873186, 2019.
[14] P. Almasan, M. Ferriol-Galmés, J. Paillisse, J. Suárez-Varela, D. Perino, D. López, A. A. P. Perales, P. Harvey, L. Ciavaglia, L. Wong, V. Ram, S. Xiao, X. Shi, X. Cheng, A. Cabellos-Aparicio, P. Barlet-Ros, Network digital twin: Context, enabling technologies, and opportunities, IEEE Communications Magazine 60 (11), 22–27. doi:10.1109/MCOM.001.2200012, 2022
[15] D. Wang, Y. Song, Y. Zhang, X. Jiang, J. Dong, F. N. Khan, T. Sasai, S. Huang, A. P. T. Lau, M. Tornatore, M. Zhang, Digital twin of optical networks: A review of recent advances and future trends, Journal of Lightwave Technology, 1–28, doi:10.1109/JLT.2024.3401419, 2024.
[16] Seattle Internet Exchange Point. https://www.seattleix.net/statistics/.
[17] P. Lechowicz, R. Goscien, R. Rumipamba-Zambrano,J. Perello, S. Spadaro, K. Walkowiak, Greenfield gradual migration planning toward spectrally-spatially flexible optical networks, IEEE Communications Magazine 57 (10), 14–19. doi:10.1109/MCOM.001.1900207, 2019
[18] S. Petale, S.-C. Lin, M. Matsuura, H. Hasegawa, S. Subramaniam, PRODIGY: A progressive upgrade approach for elastic optical networks, in: IEEE Global Communications Conference (GLOBECOM), pp. 2129–2134. doi:10.1109/ GLOBECOM54140.2023.10437935, 2023.
[19] A. Knapińska, P. Lechowicz, K. Walkowiak, Machine-learning based prediction of multiple types of network traffic, in: International Conference on Computational Science (ICCS), Springer, pp. 122–136. doi:10.1007/978-3-030-77961-0_12, 2021
[20] A. Knapińska, P. Lechowicz, W. Węgier, K. Walkowiak, Long-term prediction of multiple types of timevarying network traffic using chunk-based ensemble learning, Applied Soft Computing 130, 109694. doi:10.1016/j.asoc.2022.109694, 2022
[21] A. Knapińska, P. Lechowicz, K. Walkowiak, Prediction of multiple types of traffic with a novel evaluation metric related to bandwidth blocking, in: IEEE Global Communications Conference (GLOBECOM), pp. 2927–2932. doi:10.1109/ GLOBECOM48099.2022.10001028, 2022
[22] A. Knapińska, P. Lechowicz, S. Spadaro, K. Walkowiak, Agnostic prediction of multiple types of timevarying traffic in optical networks, in: IEEE Global Communications Conference (GLOBECOM), pp. 1131–1136. doi:10.1109/GLOBECOM54140.2023.10436763, 2023.
[23] Sandvine, The mobile internet phenomena report (May 2021), https://www.sandvine.com/download-mobile-internet-phenomena-report-2021, 2021.
[24] P. Lechowicz, A. Knapińska, A. Włodarczyk, K.Walkowiak, Traffic Weaver: semi-synthetic time-varying traffic generator based on averaged time series, https://arxiv.org/abs/2403.11388, 2024.
[25] I. Lohrasbinasab, A. Shahraki, A. Taherkordi, A. Delia Jurcut, From statistical-to machine learningbased network traffic prediction, Transactions on Emerging Telecommunications Technologies 33 (4), e4394. doi:10.1002/ETT.4394, 2022
[26] G. O. Ferreira, C. Ravazzi, F. Dabbene, G. C. Calafiore, M. Fiore, Forecasting network traffic: a survey and tutorial with open-source comparative evaluation, IEEE Access Vol. 11, 6018–6044. doi: 10.1109/ACCESS.2023.3236261, 2023
[27] A. Knapińska, R. Goścień, P. Lechowicz, K. Walkowiak, Link load prediction in an optical network with restoration mechanisms, Journal of Optical Communications and Networking 15 (5), B42–B52. doi:10.1364/JOCN.479849, 2023.
[28] S. M. Lundberg, S.-I. Lee, A unified approach to interpreting model predictions, Advances in neural information processing systems (NIPS) 30, 2017.
[29] A. Knapińska, O. Ayoub, C. Rottondi, P. Lechowicz, K. Walkowiak, Explainable artificial intelligence-guided optimization of ML-based traffic prediction, in: 28th International Conference on Optical Network Design and Modeling (ONDM), pp. 1–6, 2024.
[30] A. Knapińska, K. Półtorak, D. Poręba, J. Miszczyk, M. Daniluk, K. Walkowiak, On feature selection in short-term prediction of backbone optical network traffic, in: 26th International Conference on Optical Network Design and Modeling (ONDM), pp. 1–6, 2022.
[31] A. Knapińska, R. Kanimba, Y. Yesilyurt, K. Walkowiak, Application of ensemble regression methods in elastic optical network optimization, in: 5th Polish Conference on Artificial Intelligence (PP-RAI), pp. 1–6, 2024.
[32] K. Duszyńska, P. Polski, M. Włosek, A. Knapińska, P. Lechowicz, K. Walkowiak, XAI-guided optimization of a multilayer network regression model, in: 1st International Workshop on Trustworthy and Explainable Artificial Intelligence for Networks (TX4Nets) at the IFIP/IEEE Networking Conference, pp. 170–175, 2024.

DOI: 10.15199/59.2024.4.3

# Fale milimetrowe i terahercowe w systemach komórkowych: wykorzystanie, modelowanie propagacji i wpływ na architekturę sieci

## Millimeter and terahertz waves in cellular systems: utilization, propagation modeling and impact on network architecture

dr hab. inż. SŁAWOMIR HAUSMAN, prof. PŁ

Sławomir Hausman, Politechnika Łódzka, Instytut Elektroniki,
slawomir.hausman@p.lodz.pl

STRESZCZENIE Oczekuje się, że technologie dostępu radiowego wykorzystujące fale milimetrowe (mmWave), a w jeszcze większym stopniu terahercowe (THz), zapewnią znacznie większą niż obecnie przepustowość, zwłaszcza w obszarach o dużym natężeniu ruchu. Jednocześnie, silnie kierunkowe charakterystyki promieniowania anten, które muszą być wykorzystywane zarówno po stronie nadawczej, jak i odbiorczej łącza w celu przezwyciężenia znaczących strat absorpcyjnych w gazach atmosferycznych, dynamiczne blokowanie ścieżek propagacji przez duże statyczne i małe poruszające się obiekty, makro- i mikromobilność urządzeń użytkownika sprawia, że świadczenie niezawodnych usług za pośrednictwem tych zakresów częstotliwości jest złożonym zadaniem. Wyzwanie to jest dodatkowo komplikowane przez rodzaj spodziewanych aplikacji przewidzianych dla tych systemów, które z natury wymagają gwarantowanych parametrów jakościowych w interfejsie radiowym. W artykule omówiono wybrane zagadnienia dotyczące wykorzystania, modelowania propagacji i wpływu fal z tego zakresu na architekturę przyszłych sieci mobilnych
SŁOWA KLUCZOWE: fale terahercowe, fale milimetrowe, modelowanie propagacji, systemy komórkowe i bezkomórkowek

ABSTRACT Radio access technologies using millimeter waves (mmWave), and to an even greater extent terahertz (THz) bands, are expected to provide significantly higher throughput than today in high traffic areas. At the same time, the highly directional radiation patterns of the antennas, which must be used on both the transmit and receive sides of the link to overcome significant atmospheric absorption, the dynamic blocking of propagation paths by large static and small moving objects, and the macro- and micromobility of user equipment (UEs) make providing reliable services over these frequency bands an extremely complex task. This challenge is further complicated by the type of applications envisioned for these systems, which inherently require guaranteed quality of service at the radio interface. This paper discusses selected issues regarding the use, propagation modeling and impact of mmWave ant THz range on the architecture of future mobile networks.
KEYWORDS terahertz waves, millimeter waves, propagation modeling, cellular systems, cell-free systems

Pomijając różnice przeznaczeń częstotliwości dla poszczególnych regionów świata, można przyjąć, że kolejne generacje systemów komórkowych używają lub używały następujących zakresów częstotliwości: **1G**: 450 MHz; 900 MHz; **2G**: 850 MHz, 900 MHz, 1800 MHz, 1900 MHz; **3G**: 850 MHz, 900 MHz, 1700 MHz, 1800 MHz, 1900 MHz, 2100 MHz; **4G**: 700 MHz, 800 MHz, 1700 MHz, 1800 MHz, 1900 MHz, 2100 MHz, 2300 MHz, 2500 MHz, 2600 MHz; **5G**: tzw. Sub-6 GHz (450 MHz – 6 GHz) i fale milimetrowe (24 GHz – 52 GHz). Pokazuje to że branża komórkowa wykorzystuje pasma coraz większych częstotliwości, aby uzyskać dostęp do coraz szerszego widma i sprostać rosnącym wymaganiom w zakresie przepustowości oraz opóźnień transmisji.

Przewiduje się, że w przyszłościowych generacjach systemów łączności bezprzewodowej (6G i kolejnych) będą wykorzystywane jeszcze większe częstotliwości, tj. 100 GHz – 10 THz (co odpowiada długościom fali od 3 mm do 30 μm), które są określane jako zakres terahercowy. Czasami zakres 100 – 300 GHz określany jest jako subterahercowy. Poniżej tego zakresu znajdują się zakresy częstotliwości fal milimetrowych (tzw. mmWave) – już obecnie wykorzystywane w zastosowaniach telekomunikacyjnych oraz nietelekomunikacyjnych, np. radarach samochodowych (głównie pasmo 76–81 GHz). Własności zakresu fal subterahercowych i terahercowych są obecnie badane pod kątem możliwości wykorzystania w systemach komórkowych 6G do realizacji transmisji danych z dużą przepływnością, ponieważ udostępniają nowe pasma o szerokości dziesiątek, a nawet setek GHz [1, 2]. Warto zauważyć, że umożliwiają także zmniejszenie opóźnień transmisji, pozwalając na przesyłanie dużej liczby bitów w krótkich pakietach danych, co skraca czas buforowania tych pakietów w procesie transmisji i komutacji. Małe opóźnienia mają duże znaczenie dla zastosowań czasu rzeczywistego: układów sterowania w pętli sprzę-

żenia zwrotnego obejmującej łącze radiowe, np. dla latających pojazdów bezzałogowych, połączonych pojazdów samochodowych, przemysłu 4.0. Fale w tym zakresie długości mogą być również wykorzystywane do zastosowań nietelekomunikacyjnych, w tym radarów (nadzór obiektów i wykrywanie w innych celach, pojazdy autonomiczne, itp.) a nawet obrazowania medycznego i technicznego, co bezpośrednio wiąże się z koncepcją „communication and sensing" [3]. Uważa się, że sieci 6G pozwolą np. na rozwój holografii, bo osiągnięcie tego celu wymaga przetwarzania bardzo dużych strumieni danych w czasie zbliżonym do rzeczywistego, z przepływnością ok. Tb/s i niskimi, nieosiągalnymi jeszcze obecnie, opóźnieniami, rzędu setek a nawet tylko dziesiątek μs [4].

Osiągnięcie takich parametrów transmisyjnych w mobilnym łączu radiowym wymagać będzie rozwiązania wielu problemów wynikających ze specyfiki propagacji fal terahercowych w atmosferze, które będą wymagały uwzględnienia w architekturze przyszłych sieci. Obecnie przewiduje się, że sieci 6G będą opracowane i zaczną być wdrażane do ok. 2030 r. Istnieje już znacząca globalna konkurencja w tym zakresie, aby wpłynąć na opracowanie i wdrożenie systemów 6G w sposób odzwierciedlający interesy społeczne, gospodarcze i bezpieczeństwa regionów finansujących te prace [5]. Obecnie zaawansowane są prace przestandaryzacyjne [6].

## ZAKRESY CZĘSTOTLIWOŚCI I MODELE PROPAGACJI

ETSI TeraHertz Industry Specification Group (ISG) wydała dwa raporty dotyczące pasm terahercowych. W raporcie ETSI GR THz 001 [7] identyfikuje i opisuje przypadki użycia możliwe dzięki komunikacji terahercowej. Aspekty poruszone w dokumencie obejmują scenariusze wdrażania, potencjalne wymagania, odpowiednie środowiska operacyjne i związane z nimi charakterystyki propagacji. Dokument omawia 19 przykładowych, zróżnicowanych przypadków użycia, w których komunikacja terahercowa odgrywa główną rolę takich jak: zdalne operacje z użyciem robotów chirurgicznych, rozrywka audiowizualna w pociągach i samolotach, interaktywna immersyjna rzeczywistość rozszerzona, sterowanie czasu rzeczywistego w produkcji, pojazdy połączone, współpracujące sieci robotów np. sieci bezzałogowych statków powietrznych. Każdy przypadek użycia jest opisany według następującego schematu: opis ogólny, warunki umożliwiające realizację, schemat przepływu informacji i realizacji usług, kryteria osiągnięcia sukcesu, potencjalne wymagania ze strony sieci radiowej, środowisko fizyczne i niezbędne technologie wspomagające.

W innym raporcie – ETSI GR THz 002 [8] wskazano pasma częstotliwości będące przedmiotem zainteresowania w zakresie teraherców, w kontekście obecnej sytuacji regulacyjnej. Jest to o tyle istotne, że zakres częstotliwości od 100 GHz wzwyż jest już wykorzystywany do celów niekomunikacyjnych, np. w astrofizyce [9], co zmusza do przeanalizowania aktualnego krajobrazu regulacyjnego i zidentyfikowania pasm częstotliwości dla powszechnej łączności bezprzewodowej. Dokument [8] zawiera szczegółowy i kompleksowy przegląd zakresów częstotliwości od 100 GHz do 1 THz, z uwzględnieniem stanu regulacji w zakresie zarządzania widmem i wyzwań związanych z koegzystencją różnych służb radiokomunikacyjnych. Pomiędzy 100 GHz a 275 GHz zidentyfikowano 8 pasm o wystarczającej ciągłości, które mogą być przydzielone służbie stałej i ruchomej, co stanowi łącznie 90,7 GHz szerokości pasma. Powyżej 275 GHz zidentyfikowano interesujące pasma do celów łączności terahercowej w oparciu o koincydencję statusu regulacyjnego i korzystnych warunków propagacyjnych. Zdefiniowano koncepcję okien transmisyjnych, aby zidentyfikować przydatne zakresy częstotliwości powyżej 275 GHz. W wyniku przeprowadzonej analizy wskazano 12 interesujących pasm o szerokości 488 GHz. 91 GHz z tego zakresu zidentyfikowano jako przydatne dla służby stałej i ruchomej. Przewiduje się, że dla służby ruchomej dostępne będą pasma o łącznej szerokości ponad 150 GHz, podczas gdy w pasmach poniżej 6 GHz było to zaledwie ok. 1 GHz. Pokazuje to bardzo duży potencjał rozwojowy sieci mobilnych w kierunku usług wymagających zapewnienia nie tylko bardzo dużej przepływności dla pojedynczych użytkowników, ale także bardzo dużych wartości powierzchniowej gęstości ruchu, Jest to istotne np. dla tzw. autonomicznych pojazdów połączonych przy dużym natężeniu ruchu drogowego, co będzie wymagało bezprecedensowego poziomu niezawodności i niskich opóźnień (tj. odpowiednio powyżej 99,99999% i poniżej 1 ms), nawet w scenariuszach bardzo wysokiej mobilności (zakłada się nawet do 1000 km/h), aby zagwarantować bezpieczeństwo pasażerów, co jest wymogiem trudnym do spełnienia przy użyciu istniejących technologii [10]. Obecnie trudno jeszcze przewidzieć na ile wdrożenie systemów o takich parametrach jakościowych będzie możliwe dla całości sieci dróg i szlaków kolejowych, zwłaszcza biorąc pod uwagę konieczność zapewnienia widzialności optycznej dla kanałów terahercowych (ewentualnie wykorzystania omówionych dalej rozwiązań typu inteligentne powierzchnie odbijające).

Dokument ETSI powołuje się na zalecenie ITU-R P.676-13 [11], zatytułowane „Attenuation by Atmospheric Gases". Dostarcza ono wytycznych dotyczących przewidywania tłumienia fal radiowych spowodowanego przez gazy atmosferyczne, takie jak tlen i para wodna, w szerokim zakresie częstotliwości (do 1 THz). Ma to kluczowe znaczenie dla projektowania i działania naziemnych i satelitarnych systemów komunikacyjnych, a także aplikacji teledetekcyjnych. Kluczowe zastosowania zalecenia obejmuje obliczanie tłumienności (w dB/km) powodowanego przez gazy atmosferyczne, które zmienia się w zależności od częstotliwości, temperatury, ciśnienia i wilgotności. Pozwala to wyznaczać budżet energetyczny łącza, stosunek sygnału do szumu i niezawodność łączy komunikacyjnych. Zalecenie wspiera również zarządzanie widmem częstotliwości poprzez dostarczanie informacji o pasmach częstotliwości, w których fale mogą doświadczać znacznej absorbcji, wpływając w ten sposób na alokację i wykorzystanie za-

sobów widma z uwzględnieniem różnych specyficznych warunków klimatycznych w różnych regionach geograficznych. Zalecenie ITU-R P.676-13 można więc wykorzystać do przewidywania pasm częstotliwości („okien transmisji") przydatnych dla telekomunikacji. W tym celu wprowadzono pojęcie transmitancji, która jest definiowana jako ułamek mocy padającej fali elektromagnetycznej, która jest przenoszona przez atmosferę. Transmitancja jest podawana w procentach i może być wyprowadzona z tłumienia atmosferycznego. Tab. 1 przedstawia okna transmisji dla jednego przykładu danych wejściowych, tj. długości łącza 100 metrów na poziomie morza, dla temperatury 15°C i gęstości pary wodnej 7,5 g/m$^3$ [11]. W dokumencie źródłowym można znaleźć dane dla innych warunków. Szerokość każdego pasma jest zdefiniowana pomiędzy wartościami 1/√2 wartości szczytowej transmitancji, indywidualnie dla każdego pasma częstotliwości. Wymienione wyżej raporty ETSI i zalecenie ITU stanowią istotą podstawę prac przedstandaryzacyjnych dla komunikacji terahercowej w systemach 6G.

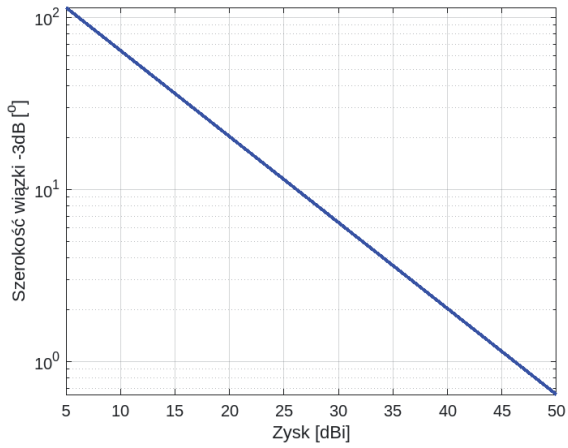
» *Tab. 1. Okna transmisyjne w pasmie THz dla długości łącza 100 m na poziomie morza, w temperaturze 15° i gęstości pary wodnej 7,5 g/m$^3$. Niektóre z zakresów mają już przeznaczenia niezwiązane ze służbą ruchomą. (Na podstawie [11])*

» *Tabl. 1. Transmission windows in the THz band for a link length of 100 m at sea level, at temperature of 15°C and a water vapor density of 7.5 g/m3 Some of the sub-bands have existing allocations unrelated to mobile service. (Based on [11])*

| Numer okna | Częstotliwość dolna [GHz] | Częstotliwość górna [GHz] | Szerokość pasma [GHz] |
|---|---|---|---|
| 1 | 100 | 180 | 80 |
| 2 | 185 | 321 | 136 |
| 3 | 328 | 369 | 41 |
| 4 | 391 | 433 | 42 |
| 5 | 457 | 488 | 31 |
| 6 | 635 | 696 | 62 |
| 7 | 811 | 892 | 81 |

Znacząco nowe problemy związane z fizyką propagacji pojawiają się już dla fal milimetrowych, które mają częstotliwości kilkukrotnie większe niż używane wcześniej pasma poniżej 6 GHz. [12, 13]. Problemy te się nasilają dla pasm terahercowych. Pierwszoplanowe są duże absorpcyjne straty propagacyjne i potrzeba stosowania anten silnie kierunkowych.

Korzystnie, jak widać z *rys. 1.*, duże wartości zysku anten implikują małe szerokości wiązki. Na przykład przy powierzchni anteny terminala rzędu 0,01 m$^2$ (np. 10 × 10 cm) i falach milimetrowych możliwe są w praktyce zyski anten rzędu 25 dBi, co odpowiada (*rys. 1*) szerokości wiązki rzędu 10°. Po stronie stacji bazowych możliwe będzie dla zakresu terahercowego uzyskiwanie zysku ponad 25 dBi. Problem można przedstawić tak: duże straty absorpcyjne dla częstotliwości terahercowych mogą być kompensowane przez duży zysk anten. To jednak implikuje bardzo wą-




» *Rys. 1. Oszacowanie szerokości wiązki anteny [o] (definiowanej dla spadku -3 dB), jako funkcja zysku anteny [dBi], z pominięciem wpływu listków bocznych i listka wstecznego oraz strat*

» *Fig. 1. Estimation of antenna beamwidth[°] (defined for the -3 dB drop), as a function of antenna gain [dBi], neglecting the influence of side lobes, back lobes and losses*

skie charakterystyki promieniowania i w konsekwencji niemal wyłącznie bezpośrednie ścieżki propagacji, dodatkowo z pomijalnie małymi składowymi odbitymi, dyfrakcyjnymi i rozproszonymi. W warunkach wnętrz budynków i środowisku miejskim wymaga to gęstego rozmieszczenia stacji bazowych (lub punktów dostępowych) i/lub dynamicznego kształtowania środowiska propagacji, co zostanie opisane w dalszej części artykułu.

W tym miejscu warto podkreślić, że w literaturze, w analizach propagacyjnych dość powszechnie błędnie interpretuje się wzór Friisa (1) pozwalający wyznaczać moc odebraną w warunkach wolnoprzestrzennych.

$$(1)\quad P_R = P_T G_T G_R \left(\frac{\lambda}{4\pi R}\right)^2 = P_T G_T G_R \left(\frac{\frac{c}{f}}{4\pi R}\right)^2$$

gdzie: $P_R$ – moc odebrana, $P_T$ – moc nadawana, $G_T$ – zysk anteny nadawczej, $G_R$ – zysk anteny odbiorczej, $\lambda$ – długość fali, $f$ – częstotliwość fali, $R$ – odległość odbiornika od nadajnika.

Z (1) łatwo jest wysnuć niepoprawny wniosek, że tłumienność w wolnej przestrzeni jest proporcjonalna do kwadratu częstotliwości. Stąd biorą się niezgodne z fizyczną rzeczywistością przewidywania, że dla fal terahercowych straty w wolnej przestrzeni są bardzo duże w porównaniu do fal milimetrowych, a tym bardziej <6 GHz. Lepszy wgląd w to zagadnienie daje zastąpienie zysku anteny odbiorczej jej efektywną powierzchnią $A_R$ (2).

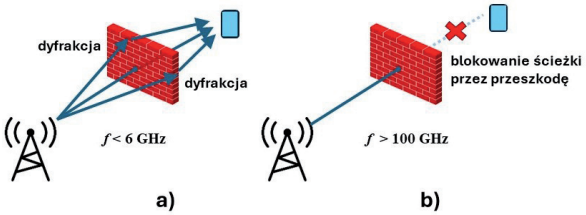
$$(2)\quad P_R = P_T G_T G_R \left(\frac{\lambda}{4\pi R}\right)^2 = P_T G_T \frac{4\pi A_R}{\lambda^2}\left(\frac{\lambda}{4\pi R}\right)^2 = \frac{P_T G_T}{4\pi}\frac{1}{R^2}A_R = S A_R$$

gdzie: $A_R$ – powierzchnia skuteczna anteny odbiorczej, S – powierzchniowa gęstość mocy w punkcie odbioru.

Jak widać w tej wersji równania znika zależność mocy odebranej od częstotliwości, która teraz zależy tylko od mocy nadawania, zysku anteny nadawczej, powierzchni skutecznej anteny odbiorczej oraz odległości odbiornika od nadajnika. Tak więc, niekorzystne cechy propagacyjne fal terahercowych wynikają z propagacji w obecności gazów atmosferycznych, a nie w wolnej przestrzeni.

Realizowalność komunikacji z wykorzystaniem zakresów fal milimetrowych i terahercowych na zewnątrz zależy od warunków atmosferycznych/środowiskowych, które obejmują gazy atmosferyczne, wilgotność, deszcz, śnieg, mgłę i liście. [14]. Podczas opadów deszczu fale są pochłaniane lub rozpraszane, co wiąże się z tym, że długość fali jest porównywalna z wielkością kropel deszczu, albo nawet od niej mniejsza. Powoduje to znaczne tłumienie sygnału określane jako tłumienie deszczowe, którego przykładowa wartość dla fal subterahercowych (300 GHz) wynosi ok. 12 dB/km, przy opadach o intensywności 25 mm/h. Opady śniegu powodują jeszcze większą tłumienność dla tej częstotliwości, a gęsta mgła ok. 7 dB/km [14].

Oprócz zalet (szerokie dostępne pasma), korzystanie z fal milimetrowych i terahercowych niesie ze sobą szereg problemów. Przyczyna leży w specyficznych cechach propagacji fal radiowych, w tym wysokich stratach propagacyjnych, absorpcji atmosferycznej i deszczowej (co omówiono wyżej), ale także niewielkim składowym dyfrakcyjnym, wyższym rozproszeniu z powodu chropowatości materiałów i wysokim stratom przenikania przez obiekty (w tym materiały budowlane). Dla fal milimetrowych i terahercowych przeszkody występujące w środowiskach propagacji zarówno we wnętrzach budynków, jak i na zewnątrz są przeważnie znacznie większe niż długość fali, co redukuje udział składowych dyfrakcyjnych w sygnale odebranym (*rys. 2*).




» *Rys. 2. Poglądowo przedstawiony udział składowych przechodzących przez przeszkody i składowych dyfrakcyjnych dla a) częstotliwości <6GHz, b) częstotliwości >100 GHz*

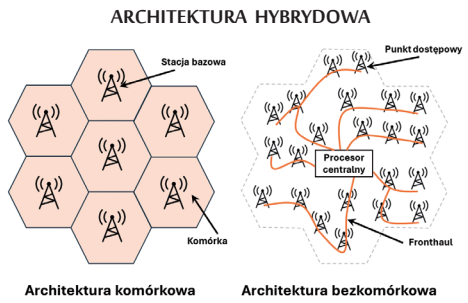
» *Fig. 2. Illustratively presented contribution of transmitted and diffracted components for a) frequencies <6 GHz, b) frequencies >100 GHz*

W praktyce, mały udział składowych dyfrakcyjnych i przechodzących przez obiekty budowlane oznacza, że komunikacja jest możliwa głównie dla przypadku widzialności optycznej nadajnika i odbiornika. Stanowi to poważne wyzwanie techniczne, wobec konieczności zachowania ciągłości komunikacji i wymusza poszukiwanie rozwiązań nieznanych z dotychczas znanych systemów komórkowych. Należy także uwzględnić dodatkowy, istotny składnik tłumienia sygnału spowodowany absorpcją w atmosferze [16, 17].

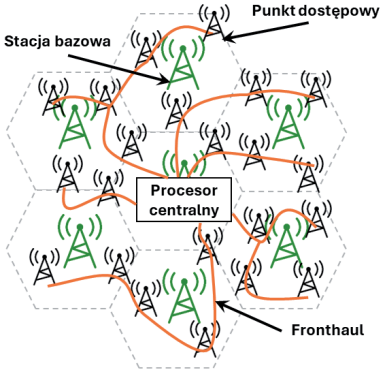
Bezprzewodowa komunikacja w paśmie terahercowym ma potencjał do realizacji ultraszybkiego i bezpiecznego transferu danych do komunikacji z i pomiędzy bezzałogowymi statkami powietrznymi (BSP). Mogłoby się wydawać, że warunki łącza z widzialnością optyczną między BSP są bardzo dobre. Jednak dla fal terahercowych turbulencje atmosferyczne spowodowane losowym przepływem powietrza prowadzą do niejednorodności przestrzennej medium propagacyjnego (której nie uwzględnia się w większości istniejących badań), co prowadzi do dodatkowych strat propagacyjnych. W [18] zaproponowano model tłumienia uwzględniający zaniki/ tłumienie spowodowane turbulencjami atmosferycznymi, gdzie zaniki wywołane turbulencjami są modelowane przez rozkład Gamma-Gamma, a tłumienie z powodu turbulencji jest funkcją wysokości lotu i częstotliwości. Uzyskane wyniki pokazują, że turbulencja prowadzi do tłumienia rzędu 10 dB przy częstotliwości mniejszej niż 1 THz i odległości mniejszej niż 10 km. Bardziej szczegółowe informacje można znaleźć w [18].

## KOMÓRKOWA I BEZKOMÓRKOWA ARCHITEKTURA SIECI

Zapotrzebowanie na obsługę ruchu dla zastosowań takich jak rzeczywistość wirtualna skłaniają do densyfikacji stacji bazowych i upowszechniania się technik massive MIMO (mMIMO) [19], a nawet Ultra Massive MIMO (UM-MIMO) [20]. Jednak nawet w gęstych architekturach komórkowych użytkownicy w pobliżu brzegu komórki są bardziej oddaleni niż inni od stacji bazowej i ich terminale są wyeksponowane na zwiększone zakłócenia wspólnokanałowe. W rezultacie mogą występować znaczne różnice w jakości usług między użytkownikami w centrum komórki i na jej brzegu. Redukcja tego problemu i zapewnienie wysokiej jakości usług dla wszystkich użytkowników są jednym z celów w przyszłych sieciach 6G. W tym kontekście pojawia się architektura sieci bezkomórkowych, która może radzić sobie z zakłóceniami międzykomórkowymi (wspólnokanałowymi) poprzez dynamiczną współpracę między wieloma punktami dostępowymi AP (ang. *Access Point*). Warto zauważyć, że w przypadku architektur bezkomórkowych zwykle nie używa się pojęcia stacji bazowych, tylko właśnie punktów dostępowych (*rys. 3*). Rozwiązania bezkomórkowe uważa się za podstawowe dla 6G. Jednak wizja ta jest trudna do osiągnięcia (zwłaszcza w krótkim czasie) ze względu na znaczne koszty wdrażania i zarządzania punktami dostępowymi na dużą skalę [21]. Przewiduje się współzależną heterogeniczną architekturę sieci komórkowej i bezkomórkowej, która integruje zalety obu [19] (*rys. 4*). Aktualne kierunki badań w tym zakresie omówiono m.in. w [22 i 21].




» *Rys. 3. Architektura komórkowa i bezkomórkowa*
» *Fig. 3. Cellular and cell-free architectures*

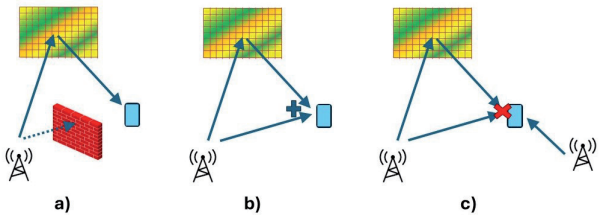



» *Rys. 4. Architektura heterogeniczna o strukturze komórkowej (głównie do realizacji kanałów sterujących i obsługi ruchu o małej przepływności) i bezkomórkowej (do realizacji kanałów ruchowych, zwłaszcza dla dużych przepływności)*
» *Fig. 4. A heterogeneous architecture with cellular (mainly for control channels and handling low bit rate traffic) and cell-free (for traffic channels, especially for high bit rates)*

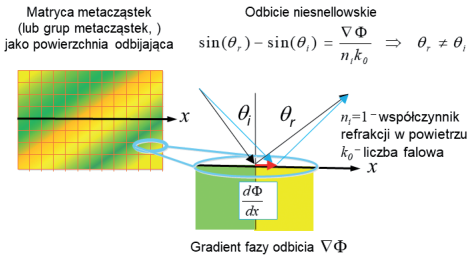
## INTELIGENTNE POWIERZCHNIE ODBIJAJĄCE

Dotychczasowe metody projektowania sieci bezprzewodowych opierają się na optymalizacji punktów końcowych łączy komunikacyjnych, np. nadajników i odbiorników. Zaproponowano w tym zakresie wiele technik, które obejmują zaawansowane schematy modulacji/kodowania, protokoły oparte na wykorzystaniu wielu anten, czy wykorzystanie zakresów częstotliwości o różnych własnościach propagacyjnych (np. inne pasma dla kanałów sygnalizacyjnych i ruchowych). Jednocześnie środowisko propagacji było dotychczas traktowane jako niedające się kontrolować. Nadrzędny paradygmat, który charakteryzuje projektowanie obecnych sieci bezprzewodowych, polega zatem na stosowaniu różnych technik kodowania, modulacji, korekcji charakterystyk kanału i wielodostępu oraz technik antenowych w nadajnikach i odbiornikach, tak aby skompensować wpływ kanału bezprzewodowego, np. dyspersję czasową i interferencje. Inteligentne powierzchnie odbijające IRS (ang. *Intelligent Reflecting Surface*) zapewniają natomiast możliwości wpływania na własności propagacyjne środowiska bezprzewodowego. IRS mogą oddziaływać na fale radiowe w trakcie propagacji, w taki sposób, że środowisko bezprzewodowe można dostosować, w celu spełnienia określonych wymagań systemowych. Środowisko bezprzewodowe nie jest zatem traktowane jako losowe i niekontrolowalne tylko jako część podlegająca projektowaniu. [23, 24].

Wykazano już, że sterowanie wiązką za pomocą inteligentnych powierzchni odbijających (IRS) [25] zapewnia potencjalnie niedrogie środki do omijania przeszkód i realizacji scenariuszy wielościeżkowych. Technologia IRS wykorzystuje regulowany reflektor oparty na metapowierzchni. Jeden ze sposobów wyjaśnienia fizycznej zasady działania IRS jest przedstawienie ich jako powierzchni mających gradient fazy odbicia i w konsekwencji umożliwiających niesnellowskie odbicie, w którym kąt odbicia nie jest równy kątowi padania (*rys. 6*)




» *Rys. 5. Przykłady zastosowania inteligentnych powierzchni odbijających: a) alternatywna ścieżka propagacji za przeszkodą, b) redukcja zaników wielodrogowych, c) redukcja interferencji wspólnokanałowych*
» *Fig. 5. Example use cases of IRSs: a) alternative propagation path behind an obstacle, b) reduction of multipath fading, c) reduction of co-channel interference*

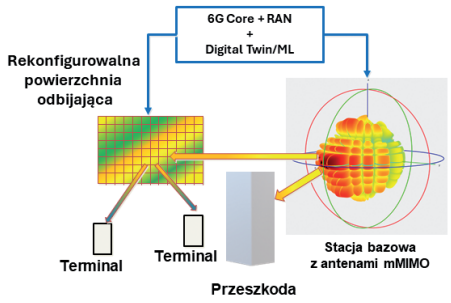



» *Rys. 6. IRS jako metapowierzchnia zgradientem fazy odbicia i w konsekwencji odbiciem niesnellowskim*
» *Fig. 6. IRS as a metasurface with reflection phase gradient resulting in non-Snellian reflection*

Dla systemów 5G w paśmie częstotliwości 18–27 GHz symulacyjna analiza zastosowania IRS została pokazana np. w [26] i [27], a praktyczna realizacja w [28] i [29]. Przykładowe scenariusze zastosowania inteligentnych powierzchni odbijających tj. alternatywną ścieżkę propagacji za przeszkodą, redukcję zaników wielodrogowych i redukcję interferencji wspólnokanałowych pokazuje *rys. 5.* Niniejszy artykuł nie omawia techniki IRS szczegółowo, a przedstawia ją wyłącznie jako jedno z rozwiązań problemów propagacyjnych dla fal milimetrowych i terahercowych.

Chociaż oczekuje się, że IRS odegrają kluczową rolę w przyszłych sieciach (właściwie nie ma dla nich alterna-

tywy), ich wdrożenie wiąże się z nowymi wyzwaniami. Wyzwania te dotyczą zarówno koniecznej dynamicznej optymalizacji w czasie rzeczywistym kierunkowej charakterystyki odbicia (*rys. 7*), jak i fizycznej implementacji odpowiednich metapowierzchni.




» *Rys. 7. Schematyczne ujęcie łącznej dynamicznej optymalizacji charakterystyk anten mMIMO i inteligentnych powierzchni odbijających IRS*
» *Fig. 7. A concept of the combined dynamic optimization of the mMIMO antenna pattern and the IRS reflection pattern*

Masowe zastosowanie IRS w sieciach 6G wydaje się obecnie warunkiem koniecznym skutecznego wykorzystania częstotliwości terahercowych w sieciach bezprzewodowych, zarówno we wnętrzach budynków, jak i na zewnątrz.

## KOMUNIKACJA I TELEDETEKCJA

Koncepcja integracji komunikacji i teledetekcji ISAC (ang. *Integrated Sensing and Communications*) w sieciach 6G i następnych generacji odnosi się do integracji funkcji lokalizacji i teledetekcji z funkcjami komunikacyjnymi. Takie funkcje nie tylko umożliwią nowe zastosowania, ale także stanowią środek do wspierania i poprawy funkcji komunikacyjnych, np. przez kierowanie wiązek anten mMIMO lub inteligentnych powierzchni odbijających w stronę zlokalizowanych użytkowników lub ich grup. Wspólne wykrywanie i komunikację uważa się za kluczowe technologię i wartość dodaną 6G. Obszerne omówienie tej tematyki można znaleźć w [30] Wizja zintegrowanych sieci ISAC obejmuje wykorzystanie technik przetwarzania sygnałów, optymalizacji i uczenia maszynowego, aby stały się one rzeczywistością w kontekście 6G. Dwufunkcyjne sieci ISAC oferują doskonałą synergię dzięki komunikacji wspomaganej wykrywaniem i wykrywaniu wspomaganemu komunikacją [31].

Radary samochodowe już obecnie umożliwiają realizację funkcji takich jak adaptacyjny tempomat i półautonomiczna jazda. Dalszy rozwój tych systemów przy użyciu fal terahercowych w znacznym stopniu przyczyni się do zwiększenia ich rozdzielczości kątowej i odległościowej [15]. Radary impulsowe i radary z modulowaną częstotliwością fali ciągłej FMCW (ang. *Frequency Modulated Continuous Wave*) to dwa podejścia do szacowania odległości i prędkości obiektów. Radary typu FMCW są bardziej popularne w zastosowaniach motoryzacyjnych. Tutaj zarówno wąskie wiązki dla anten terahercowych, jak i duża szerokość pasma sygnału radarowego w naturalny sposób zwiększą dokładność pomiaru odległości i prędkości w porównaniu z obecnie rozpowszechnionymi radarami pracującymi w paśmie 76 – 81 GHz, co jest potrzebne w realizacji pojazdów w pełni autonomicznych.

Warto zauważyć, że już fale w zakresach <6 GHz, pochodzące z istniejących typowych stacji bazowych 5G, pozwalają wykrywać przy użyciu koncepcji pasywnego radaru bistatycznego samochody i inne obiekty [32]. Zastosowanie tej idei na częstotliwościach terahercowych poprawi rozdzielczość i prawdopodobnie stanie się jedną z usług 6G.

Fale terahercowe, zależnie od częstotliwości, są w stanie przenikać przez różne materiały nieprzewodzące, np. tworzywa sztuczne, tkaniny, papier, ceramikę. Pozwala to na wykrywanie ukrytych obiektów, wad strukturalnych i warstw pod powierzchniami, dzięki czemu jest przydatne np. w kontroli bezpieczeństwa, kontroli jakości, monitorowaniu procesów. i charakterystyce materiałów [33]. Warto zauważyć, że promieniowanie w tym zakresie nie jest jonizujące i w związku z tym jest powszechnie uważane za bezpieczne dla organizmów żywych, w tym ludzi. Dodatkową zaletą jest niski poziom zakłóceń środowiskowych, np. w porównaniu do światła lub podczerwieni. Pozwala to na realizację wykrywania w środowiskach zewnętrznych lub w niekorzystnych warunkach (zadymienie, mgła), rozszerzając zastosowania w zakresie teledetekcji, monitorowania atmosfery i kontroli bezpieczeństwa. W przeciwieństwie do mniejszych częstotliwości fale terahercowe oddziałują z cząsteczkami materii w charakterystyczny sposób umożliwiając identyfikację i analizę substancji chemicznych, w tym materiałów wybuchowych [34 i 3].

## PODSUMOWANIE

Fale milimetrowe i terahercowe będą stanowić podstawę przyszłego dostępu radiowego 6G, zapewniając zwielokrotnione w stosunku do 5G zasoby widmowe w interfejsie radiowym. Systemy komórkowe 6G i kolejnych generacji będą wykorzystywać wybrane pasma z zakresu częstotliwości 100 – 1000 GHz, które nie tylko oferuje nieosiągalne dotychczas zasoby widmowe pozwalające na uzyskiwanie przepływności nawet rzędu Tb/s oraz opóźnień rzędu 10–100 µs. Możliwe stanie się połączenie komunikacji i teledetekcji w ramach tej samej infrastruktury. Oferowane będą usługi takie jak wykrywanie obiektów i obecności niektórych substancji, lokalizacja i obrazowanie.

Silna absorpcja atmosferyczna, wąskie wiązki promieniowania anten i związane z tym skutki mobilności i mikromobilności użytkowników, sprawiają, że zapewnienie oczekiwanego poziomu jakości usług będzie trudnym zadaniem, wymagającym m.in. opracowania nowych mechanizmów utrzymania ciągłości sesji. W złożonych środowiskach propagacji, takich jak wnętrza budynków i architektura miejska nie jest możliwa realizacja łączy radiowych na częstotliwościach fal milimetrowych i terahercowych bez widzialności

optycznej lub bez zastosowania anten mMIMO oraz inteligentnych powierzchni odbijających. Opracowanie takich powierzchni na poziomie umożliwiającym ich masową, opłacalną ekonomicznie produkcję jest znaczącym wyzwaniem.

Zwiększona absorpcja atmosferyczna podczas opadów deszczu, czy śniegu drastycznie zmniejsza zasięg łączy terahercowych na zewnątrz budynków i będzie prowadzić do obniżenia jakości usług. Nie da się całkowicie wyeliminować skutków zjawisk propagacyjnych, a praktyczne techniki ich ograniczania muszą być dopiero opracowane.

Wprowadzenie fal radiowych milimetrowych i terahercowych częściowo rozwiąże problemy związane z obecnym niedoborem widma, ale ich w pełni nie wyeliminuje ze względu na potrzebę korzystania z tzw. pasm zasięgowych, np. 700–900 MHz (głównie dla kanałów sterujących), tak jak w obecnych systemach 5G. Dlatego, pomimo dużego potencjału, nie należy się spodziewać, aby pasmo THz mogło całkowicie zastąpić pasma <6 GHz, które są wykorzystywane w dotychczasowych generacjach sieci łączności komórkowej.

Wobec ograniczonych zasięgów łączności z wykorzystaniem fal milimetrowych, a w jeszcze większym stopniu terahercowych, oczekuje się, że architektury bezkomórkowe będą odgrywały ważną rolę w sieciach następnych generacji. Istnieją tu jednak praktyczne trudności, np. potrzeba znaczącej densyfikacji punktów dostępowych, co stawia pytania o koszty budowy sieci 6G. Należy się spodziewać, że docelowe systemy będą heterogeniczne (komórkowe i bezkomórkowe) oraz od siebie współzależne.

Obecnie stosowane rozwiązania dostępowe byłyby nieadekwatne do w przyszłych generacji ze względu na efekty blokowania i mikromobilności użytkowników. Tych wyzwań nie można wyeliminować wyłącznie za pomocą funkcji warstwy fizycznej lub łącza i konieczne będzie wprowadzenie funkcji sieciowych typu wielopołączeniowości (ang. *multiconnectivity*). Pozwoli to przy okazji uzyskać zwiększoną niezawodność (stabilność połączeń), większe przepływności, zmniejszone opóźnienia (optymalizacja wg. najszybszej ścieżki), płynne przełączanie.

Wobec globalnej potrzeby ograniczania zużycia energii, nowy interfejs radiowy wykorzystujący fale terahercowe powinien sprzyjać zwiększonej wydajności energetycznej (J/b) z uwzględnieniem energii zużywanej przez wszystkie elementy sieci. Konieczna jest kontynuacja prac badawczych w zakresie charakteryzowania i modelowania kanałów terahercowych. Barierą wymagającą dopiero pokonania jest też opracowywanie przystępnych cenowo anten i urządzeń dla tych zakresów częstotliwości. ●

## LITERATURA


[1] Petrov V., Kurner T., and Hosako I.: *IEEE 802.15.3d: First standardization efforts for sub-terahertz band communications towards 6G*, IEEE Commun. Mag., vol. 58, nr 11, s. 28-33, Nov. 2020.

[2] Polese M., Jornet J. M., Melodia T., and Zorzi M.: *Toward end-to-end, full-stack 6G terahertz networks*, IEEE Commun. Mag., vol. 58, no. 11, pp. 48–54, Nov. 2020.

[3] Sarieddeen H. et al., *Next generation Terahertz communications: A rendezvous of sensing, imaging, and localization*, IEEE Commun. Mag., vol. 58, no. 5, pp. 69 – 75, May 2020.

[4] Moltchanov D., Sopin E., Begishev V., Samuylov A., Koucheryavy Y., and Samouylov K.: *A Tutorial on Mathematical Modeling of 5G/6G Millimeter Wave and Terahertz Cellular Systems*, IEEE Communications Surveys & Tutorials, vol. 24, no. 2, pp. 1072-1116, Secondquarter 2022, doi: 10.1109/COMST.2022.3156207

[5] Commerce Spectrum Management Advisory Committee (CSMAC), *Report of Subcommittee on 6G*, Final Report, December 2023.

[6] *ITU-R Framework for IMT-2030: Review and Future Direction*, NGMN Alliance

[7] ETSI GR THz 001 V1.1.1: *TeraHertz modeling (THz); Identification of use cases for THz communication systems*, 2024-01.

[8] ETSI GR THz 002,V1.1.1: *TeraHertz technology (THz); Identification of frequency bands of interest for THz communication systems*, 2024-03.

[9] Gurvits, L.I., Paragi, Z., Casasola, V. et al.: *THEZA: TeraHertz Exploration and Zooming-in for Astrophysics*, Experimantal Astronomy 51, 559–594, 2021, **https://doi.org/10.1007/s10686-021-09714-y**

[10] Giordani M., Polese M., Mezzavilla M., Rangan S., and Zorzi M.: *Toward 6G Networks: Use Cases and Technologies*, IEEE Communications Magazine, vol. 58, no. 3, pp. 55-61, March 2020, doi: 10.1109/MCOM.001.1900411.

[11] Recommendation ITU-R P.676-13, *Attenuation by atmospheric gases and related effects*, P Series Radiowave propagation, 08/2022.

[12] Rangan S., Rappaport T. S., and Erkip E.: *Millimeter-Wave Cellular Wireless Networks: Potentials and Challenges*, Proceedings of the IEEE, vol. 102, no. 3, pp. 366-385, March 2014, doi: 10.1109/JPROC.2014.2299397.

[13] Lin Z., Du X., Chen H. -H., Ai B., Chen Z., and Wu D.: *Millimeter-Wave Propagation Modeling and Measurements for 5G Mobile Networks*, IEEE Wireless Communications, vol. 26, no. 1, pp. 72-77, February 2019, doi: 10.1109/MWC.2019.1800035

[14] Farooq U. and Lokam A.: *Performance analysis of mmWave/subterahertz communication link for 5G and B5G mobile networks*, *Frequenz* 77, no. 11-12 (2023): 599-606. **https://doi.org/10.1515/freq-2023-0024**

[15] Jiang S., Charan G., and Alkhateeb A.: *LiDAR aided future beam prediction in real-world millimeter wave V2I communications*, IEEE Wireless Communications Letters, vol. 12, no. 2, pp. 212–216, 2022.

[16] Smith E. K.: *Centimeter and millimeter wave attenuation and brightness temperature due to atmospheric oxygen and water vapor*, Radio Sci., vol. 17, no. 6, pp. 1455–1464, Nov./Dec. 1982.

[17] Liebe H. J. and Layton D. H.: *Millimeter-wave properties of the atmosphere: Laboratory studies and propagation modeling,* NASA STI, Washington, DC, USA, Recon Rep. N 88, 1987, Art. no. 21387. Weijun Gao, Chong Han, Zhi Chen: *Attenuation and Loss of Spatial Coherence Modeling for Atmospheric Turbulence in Terahertz UAV MIMO Channels,* arXiv:2308.10424v2, 2023.

[18] Chen B. Ji, Z., Mumtaz S., Han C., Li C., Wen H., and Wang D.: *A vision of IoV in 5G HetNets: Architecture, key technologies, applications, challenges, and trends*, IEEE Network, vol. 36, no. 2, pp. 153–161, Mar. 2022.

[19] Cui M., Wu Z., Lu Y. et al.: *Near-Field MIMO Communications for 6G: Fundamentals Challenges Potentials and Future Directions*, IEEE Communications Magazine, vol. 61, no. 1, pp. 40-46, 2023.

[20] Kim T., Kim H., Choi S., and Hong D.: *How Will Cell-Free Systems Be Deployed?*, IEEE Communications Magazine, vol. 60, no. 4, pp. 46-51, April 2022, doi: 10.1109/MCOM.001.2100533.

[21] Zhang Y., Hu Q., Peng M., Liu Y., Zhang G., and Jiang T.: *Interdependent Cell-free and Cellular Networks: Thinking the Role of Cell-free Architecture for 6G*, IEEE Network, doi: 10.1109/MNET.2023.3336218.

[22] Di Renzo M., Zappone, A., Debbah M., Alouini M.S., Yuen C., De Rosny J., Tretyakov S.: *Smart radio environments empowered by reconfigurable intelligent surfaces: How it works, state of research, and the road ahead*, IEEE J. Sel. Areas Commun. 2020, 38, 2450–2525.

[23] E Silva JDS, Ribeiro JAP, Adanvo VF, Mafra SB, Mendes LL, Li Y, de Souza RAA.: *A Survey on the Impact of Intelligent Surfaces in the Terahertz Communication Channel Models,* Sensors (Basel). 2023 Dec 20;24(1):33. doi: 10.3390/s24010033. PMID: 38202894; PMCID: PMC10780764.

[24] Yuanwei Liu, Xiao Liu, Xidong Mu, Tianwei Hou, Jiaqi Xu, Marco Di Renzo, Naofal Al-Dhahir: *Reconfigurable Intelligent Surfaces: Principles and Opportunities*, IEEE Communications Surveys and Tutorials, VOL. 23, NO. 3, THIRD QUARTER 2021Rotshild D., Rahamim E., Abramovich A.: *Innovative reconfigurable metasurface 2-D Beam-Steerable reflector for 5G wireless communication*, Electronics, 2018.

[25] Rahamim E., Rotshild E., Abramovich A.: *Performance Enhancement of Reconfigurable Metamaterial Reflector Antenna by Decreasing the Absorption of the Reflected Beam*, Applied Science, 2021. Rotshild D., Abramovich A.: *Realization and validation of continuous tuneable metasurface for high resolution beam steering reflector at K-band frequency*, International Journal of RF Microwave Computer Aided Eng. 2021.

[26] Abramovich A., Rozban D., Rotshild D., Rahamim E., Barom A., Yosef R., Bhanam L.: *Steer by Image Technology for Intelligent Reflecting Surface 2 based on Reconfigurable Metasurface beyond 5G communication*, Crystals, 2022.

[27] Jiang W. et al.: *Terahertz Communications and Sensing for 6G and Beyond: A Comprehensive Review*, IEEE Communications Surveys & Tutorials, doi: 10.1109/COMST.2024.3385908.

[28] Demirhan U. and Alkhateeb A.: *Integrated sensing and communication for 6G: Ten key machine learning roles*, arXiv:2208.02157, 2022.

[29] Samczyński P., Abratkiewicz K., Płotka M., Zieliński T. P., Wszołek J., Hausman S., Korbel P., Księżyk A.: *5G Network-Based Passive Radar*, IEEE Transactions on Geoscience and Remote Sensing, vol. 60, pp. 1-9, 2022, Art no. 5108209, doi: 10.1109/TGRS.2021.3137904Zandonella C.: *Terahertz imaging: T-ray specs*, Nature, vol. 424, no. 6950, p. 721, Aug. 2003.

[30] Abbasi Q. H. et al.: *Nano-communication for biome-dical applications: A review on the state-of-the-art from physical layers to novel networking concepts*, IEEE Access, vol. 4, pp. 3920 – 3935, Jul. 2016.

DOI: 10.15199/59.2024.4.4

# KRAJOWE LABORATORIUM SIECI I USŁUG PL 5G: KIERUNKI BADAŃ I PERSPEKTYWY ROZWOJU TECHNIKI 5G/6G

## 5G NATIONAL LABORATORY: PERSPECTIVE AND RESEARCH DIRECTIONS

dr hab. inż. Andrzej Bęben[1], dr inż. Maciej Sosnowski[1], mgr inż. Witold Jóźwiak[1], prof. dr hab. inż. Józef Woźniak[2], dr inż. Krzysztof Gierłowski[2], dr inż. Michał Hoeft[2], dr hab. inż. Marek Natkaniec[3], dr hab. inż. Piotr Boryło[3], mgr inż. Bartosz Belter[4], mgr inż. Maksymilan Furmann[4], dr inż. Patryk Schauer[5], dr inż. Łukasz Falas[5], mgr inż. Arkadiusz Warzyński[5], mgr inż. Igor Michalski[6], dr inż. Dariusz Więcek[6]

[1] Politechnika Warszawska, Warszawa, {andrzej.beben, maciej.sosnowski, witold.jozwiak}@pw.edu.pl

[2] Politechnika Gdańska, Gdańsk, {jozef.wozniak, krzysztof.gierlowski, michal.hoeft}@pg.edu.pl

[3] Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie, Kraków, {natkanie, piotr.borylo}@agh.edu.pl

[4] Poznańskie Centrum Superkomputerowo-Sieciowe, Poznań, {bartosz.belter, mfurmann}@man.poznan.pl

[5] Politechnika Wrocławska, Wrocław, {patryk.schauer, lukasz.falas, arkadiusz.warzynski}@pwr.edu.pl

[6] Instytut Łączności – Państwowy Instytut Badawczy, Wrocław, {i.michalski, d.wiecek}@il-pib.pl

STRESZCZENIE Artykuł przedstawia unikatową infrastrukturę badawczą PL 5G opracowaną w ramach projektu „Krajowe laboratorium sieci i usług 5G wraz z otoczeniem" oraz kierunki badań dotyczących techniki 5G oraz przyszłej sieci 6G. Laboratorium umożliwia prowadzenie praktycznych eksperymentów, w środowisku zbliżonym do warunków sieci operatorskiej, dotyczących rozwoju techniki 5G/6G, a także szerokiego spektrum jej zastosowań w środowiskach terenowych, tj. morskim, lotniczym, przemysłowym czy miejskim. Przedstawiono również przykładowe eksperymenty wykorzystujące rozważaną infrastrukturę.
SŁOWA KLUCZOWE sieci 5G i 6G, infrastruktura badawcza, eksperymenty

ABSTRACT The article presents the unique infrastructure of the National Laboratory for Advanced 5G Research (PL 5G) and the research directions for beyond 5G and future 6G systems. The laboratory enables practical experiments in an environment similar to the operator's network regarding the development of 5G/6G technology and a wide range of its applications in maritime, aviation, industrial, and urban environments. We also present some exemplary experiments to illustrate infrastructure capabilities.
KEYWORDS: 5G/6G technology, research infrastructure, experiments

Nie ulega wątpliwości, iż technika piątej generacji (5G) systemów komunikacji mobilnej stanowi istotny krok w ich rozwoju [1]. Główne cechy wyróżniające sieci 5G to nowe techniki radiowe pozwalające na zwiększenie przepływności bitowej oferowanej użytkownikom przy jednoczesnej większej efektywności wykorzystania pasma radiowego oraz nowe usługi bazujące na trzech podstawowych scenariuszach obsługi, tj. eMMB (ang. *Enhanced Mobile Broadband*) przeznaczonych głównie dla aplikacji wymagających dużych przepływności, URLLC (ang. *Ultra Reliable Low Latency Communications*) dedykowanych dla aplikacji wrażliwych na opóźnienia i wymagających dużej niezawodności, czy też mMTC (ang. *Massive Machine Type Communications*) zaprojektowanych dla zastosowań Internetu Rzeczy. Zmniejszenie opóźnienia przekazu danych osiągnięto między innymi dzięki wykorzystaniu techniki obliczeń na brzegu sieci (ang. *edge/fog computing*). Istotną cechą systemów 5G jest również ich ewolucja w kierunku rozwiązań programowych, bazujących na koncepcji wirtualizacji funkcji sieciowych NFV (ang. *Network Functions Virtualization*), która pozwala na rozszerzenie funkcjonalności sieci, zmniejszenie kosztów działania dzięki wykorzystaniu rozwiązań chmurowych, a także otwarcie infrastruktury na nowe podmioty, m.in. operatorów sieci prywatnych 5G, dostawców usług czy oprogramowania. Rozwój i badania nowych generacji sieci mobilnych trwają dalej i obecnie są one definiowane jako systemy 6G. Główne wyzwania badawcze [2], [3], [4] dotyczą wykorzystania fal milimetrowych i częstotliwości sub-terahercowych, systemów massive MIMO, zastosowania metod sztucznej inteligencji, uczenia ma-

szynowego oraz cyfrowego odwzorowania rzeczywistości (ang. *digital twins*), a także wykorzystania zintegrowanej infrastruktury sieciowo-obliczeniowej ECC (ang. *edge cloud continuum*) oraz zapewnienia bezpieczeństwa bazując na metodach kwantowych.

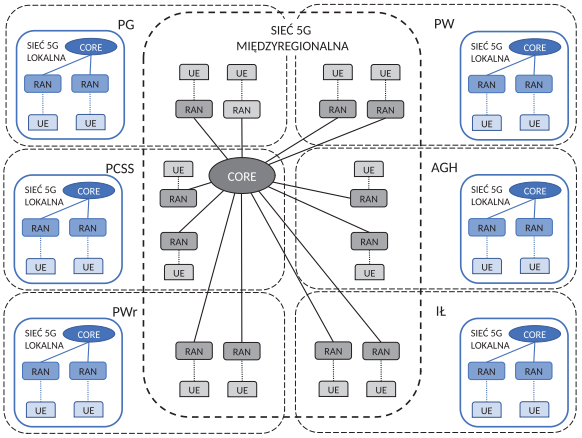
Należy podkreślić, że opracowanie nowych metod, algorytmów dla systemów 5G/6G, czy też nowych usług oferowanych w tych systemach wymaga przeprowadzenia eksperymentów dotyczących oceny efektywności, współdziałania z obecną infrastrukturą czy też oceny podatności i bezpieczeństwa proponowanych rozwiązań. Takich testów nie można przeprowadzić w sieciach operatorskich. Z tego względu na świecie pojawiły się inicjatywy budowy infrastruktur badawczych stymulujących rozwój techniki 5/6G, czego najlepszym europejskim przykładem jest inicjatywa SLICES (ang. *Scientific Large Scale Infrastructure for Computing/Communication Experimental Studies*) [5]. Udostępnienie infrastruktury o podobnej funkcjonalności krajowym ośrodkom badawczym i naukowym oraz przemysłowi, a także połączenie jej z europejskimi inicjatywami stanowiło główną motywację dla zbudowania „Krajowego laboratorium sieci i usług 5G" (PL 5G) [6]. Laboratorium to jest dużą, unikatową w skali kraju infrastrukturą badawczą znajdującą się na Polskiej Mapie Infrastruktur Badawczych, przeznaczoną do realizacji praktycznych eksperymentów dotyczących nowych technik i rozwiązań w obszarze sieci i usług 5G/5G+ oraz przyszłych sieci 6G, a także ich wykorzystania w wielu obszarach zastosowań.

Organizacja artykułu jest następująca: w rozdziale 2 została przedstawiona charakterystyka infrastruktury PL 5G obejmująca jej architekturę, wyposażenie, wykorzystywane częstotliwości oraz przeznaczenie opracowanych laboratoriów. Oferowane usługi i obszary badawcze przedstawiono w rozdziale 3. Rozdział 4 zawiera opis przykładowych eksperymentów, które przeprowadzono z wykorzystaniem infrastruktury PL 5G, zaś w rozdziale 5 podsumowano artykuł.

## OGÓLNA CHARAKTERYSTYKA

Infrastruktura PL 5G została opracowana przez konsorcjum jednostek naukowych: (1) Politechnika Warszawska (PW) – lider konsorcjum, (2) Instytut Łączności – Państwowy Instytut Badawczy (IŁ-PIB), (3) Politechnika Gdańska (PG), (4) Politechnika Wrocławska (PWr), (5) Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie (AGH) oraz (6) Instytut Chemii Bioorganicznej PAN Poznańskie Centrum Superkomputerowo-Sieciowe (PCSS).

Laboratorium PL 5G umożliwia przeprowadzanie eksperymentów w dedykowanych środowiskach testowych sieci 5G, utworzonych w ramach zasobów infrastruktury przedstawionej na Eksperymenty mogą być zestawiane: 1) w ogólnopolskiej sieci międzyregionalnej 5G, zlokalizowanej w czterech miastach, tj. w Gdańsku, Krakowie, Poznaniu i Wrocławiu, 2) w postaci wydzielonej sieci 5G, tzw. „network slice", utworzonej w sieci międzyregionalnej, lub 3) w postaci prywatnych sieci 5G utworzonych w poszczególnych lokalizacjach infrastruktury PL 5G..




» *Rys. 1. Schemat infrastruktury PL 5G*
» *Fig. 1. PL 5G infrastructure diagram*

Eksperymenty mogą być zestawiane: 1) w ogólnopolskiej sieci międzyregionalnej 5G, zlokalizowanej w czterech miastach, tj. w Gdańsku, Krakowie, Poznaniu i Wrocławiu, 2) w postaci wydzielonej sieci 5G, tzw. „network slice", utworzonej w sieci międzyregionalnej, lub 3) w postaci prywatnych sieci 5G utworzonych w poszczególnych lokalizacjach infrastruktury PL 5G.

Konfiguracja dedykowanej dla danego eksperymentu instancji sieci 5G jest definiowana przez użytkownika „na żądanie" za pomocą Systemu Zarządzania Eksperymentami. W ramach konfiguracji eksperymentu użytkownik specyfikuje wykorzystywane usługi i urządzenia obejmujące m.in. stacje bazowe wraz z terminalami, rdzeń sieci 5G, wymagane urządzenia pomiarowe, a także zasoby obliczeniowe wymagane dla uruchomienia testowanych usług. Istotną cechą laboratorium jest zapewnienie zdalnego dostępu do infrastruktury PL 5G, co oznacza, że cały proces zestawienia eksperymentu, konfiguracji urządzeń, a następnie przeprowadzenia testów i analizy wyników może być realizowany w sposób zdalny.

## WYPOSAŻENIE LABORATORIUM

Infrastruktura PL 5G oferuje elementy sieci 5G pochodzące zarówno od producentów rozwiązań klasy operatorskiej, jak również producentów rozwiązań eksperymentalnych, częściowo otwartych, zapewniających dostęp do kodów źródłowych. Z tego względu infrastruktura umożliwia prowadzenie testów rozwiązań komercyjnych oraz badań dotyczących własnych rozszerzeń. Zaprojektowana infrastruktura badawcza PL 5G jest zgodna z architekturą sieci 5G, w większości przypadków w trybie sieci 5G SA (ang. *Standalone*) i składa się z trzech powiązanych laboratoriów:

## LABORATORIUM SIECI 5G

Obejmuje ono: a) radiowe sieci dostępowe RAN (ang. *Radio Access Network*), które zbudowano, wykorzystując: stacje bazowe gNB i głowice radiowe 5G zewnętrzne i we-

wnątrzbudynkowe takich producentów jak Nokia i Amarisoft, rozwiązania Open RAN firmy Radisys, a także rozwiązania bazujące na urządzeniach radia programowalnego SDR/OAI (ang. *Software Defined Radio/Open Air Interface*), b) różne rdzenie sieci 5GC (ang. *5G core*) działające w trybie SA i NSA (ang. *Non Standalone*), które zostały zbudowane wykorzystując komercyjne rozwiązania firmy Nokia, a także eksperymentalne rdzenie firmy Fraunhofer oraz Amarisoft, c) brzegowe chmury obliczeniowe z urządzeniami zgodnymi ze standardem ETSI MEC (ang. *Multiaccess Edge Computing*), d) ogólnopolską, dedykowaną sieć szkieletową zbudowaną w oparciu o infrastrukturę światłowodową sieci PIONIER, e) prywatną chmurę obliczeniową oferującą zasoby obliczeniowe dla uruchomienia wielu instancji sieci 5G umożliwiających prowadzenie eksperymentów w rozproszonej infrastrukturze. Laboratorium sieci 5G obejmuje również urządzenia programowalne i akceleratory sprzętowe GPU/DPU wspierające przetwarzanie danych, w szczególności akceleratory wspierające metody bazujące na sztucznej inteligencji. Istotną cechą rozwiązań zastosowanych w infrastrukturze PL 5G jest zachowanie otwartych interfejsów programowych oraz, w przypadku rozwiązań eksperymentalnych, zapewnienie dostępu do kodów źródłowych umożliwiających rozszerzenie funkcjonalności systemu.

## LABORATORIUM SYMULATORÓW I APARATURY POMIAROWEJ 5G

Laboratorium to udostępnia aparaturę i oprogramowanie umożliwiające: a) prowadzenie powtarzalnych eksperymentów w kontrolowanym środowisku radiowym utworzonym przez komory (ang. *shieldbox*) i namioty izolujące sygnały radiowe, programowalne tłumiki i przełączniki sygnałów radiowych, b) realizację pomiarów dotyczących propagacji sygnałów radiowych, pomiarów anten i kompatybilności elektromagnetycznej, wykorzystując komorę bezodbiciową hybrydową, emulatory kanałów radiowych i analizatory widma, c) badanie wydajności sieci 5G i jej elementów dotyczących płaszczyzny sterowania i przekazu danych wykorzystując analizatory/generatory i emulatory sieci 5G, np. Spirent Landslide, STC, IXIA IxLoad, d) badanie bezpieczeństwa i podatności systemów 5G wykorzystując narzędzia, np. Spirent CyberFlood/Avalanche. Ponadto, laboratorium dysponuje emulatorami użytkowników i elementów sieci 5G oraz symulatorami sieci 5G umożliwiającymi prowadzenie badań wydajności, skalowania oraz bezpieczeństwa w dużych systemach.

## LABORATORIUM OTOCZENIA SIECI 5G

Zawiera ono urządzenia i oprogramowanie dla tworzenia rozwiązań sieciowych, platform i aplikacji bazujących na technice 5G. W szczególności wyposażenie infrastruktury PL 5G jest dedykowane do prowadzenia badań dotyczących zastosowania sieci 5G w obszarze Internetu Rzeczy, zastosowań multimedialnych, w tym rozszerzonej (AR), mieszanej (MR), czy wirtualnej rzeczywistości (VR), Przemysłu 4.0, a także zastosowań 5G w specyficznych środowiskach takich jak środowisko morskie, lotnisko, czy środowisko miejskie.

Infrastruktura PL 5G jest zbudowana z sześciu węzłów (lokalnych laboratoriów) zlokalizowanych w siedzibach partnerów projektu. Węzły te są połączone dedykowaną siecią światłowodową 10/100 Gbit/s, wykorzystującą zasoby sieci PIONIER. Rozproszony charakter infrastruktury PL 5G umożliwia prowadzenie badań w warunkach zbliżonych do warunków panujących w sieciach operatorskich. Należy podkreślić, że infrastruktura PL 5G zapewnia izolację zasobów; najczęściej dla danego eksperymentu są udostępniane dedykowane instancje sieci 5G, co umożliwia prowadzenie badań w różnych warunkach ruchowych, w tym w sytuacji występowania przeciążenia, niedostępności zasobów lub symulowanych ataków i uszkodzeń jej elementów. Badania tego typu nie mogą być prowadzone w sieciach operatorskich.

## WYKORZYSTYWANE CZĘSTOTLIWOŚCI

W sieci PL 5G dla emisji testowych wykorzystano częstotliwości radiowe służące do pracy w sieciach 5G NR. Zasadniczo wykorzystywane są dwa podstawowe zakresy częstotliwości pracy sieci 5G NR: FR1 (ang. *Frequency Range 1*) – częstotliwości poniżej 7125 MHz oraz FR2 – częstotliwości powyżej 24,25 GHz. Zakres FR1 jest odpowiedni do pracy na rozległych obszarach (duże zasięgi stacji), podczas gdy częstotliwości zakresu FR2 wykorzystywane są do emisji lokalnych (małe zasięgi), gdy wymagana jest bardzo duża przepustowość (bardzo szerokie kanały radiowe). Ponadto, wykorzystywane są także emisje w pasmach nielicencjonowanych ISM (tj. 2,4 GHz, 5 GHz). W przypadku zakresu FR1 dla każdej lokalizacji emisji dokonano uzgodnienia z UKE odpowiednich kanałów częstotliwości w paśmie C (zakres 3,4 ÷ 4,2 GHz), w którym głównie pracują na świecie stacje 5G NR, a w przypadku zakresu FR2 odpowiednich kanałów pasm milimetrowych (24,25 ÷ 29,5 GHz). Dodatkowo pozyskano lokalnie niewielkie zasoby niskich częstotliwości (< 3 GHz) do celów realizacji emisji w standardach 3GPP (CAT1, NB IoT) dla systemów IoT pracujących na duże odległości.

Należy również podkreślić, że laboratorium PL 5G oferuje też kontrolowane środowiska radiowe (komora bezodbiciowa, shieldbox'y i namioty izolujące sygnały radiowe), umożliwiające wykorzystanie dowolnych częstotliwości radiowych z zakresów FR1 i FR2 bez konieczności uzyskiwania pozwoleń UKE.

## LABORATORIA I ICH PRZEZNACZENIE

W tym rozdziale przedstawiono charakterystykę laboratoriów tworzących infrastrukturę PL 5G.

## Laboratorium międzyregionalne

Laboratorium międzyregionalne zostało zaprojektowane głównie dla prowadzenia eksperymentów dotyczących nowych usług i zastosowań świadczonych dzięki wykorzystaniu techniki 5G. Wyróżniającą cechą tego laboratorium jest zapewnienie warunków zbliżonych do sieci operatorskich działających w trybie 24h/365. Z tego względu laboratorium zostało zbudowane w oparciu o komercyjne rozwiązanie firmy Nokia CMU (ang. *Compact Mobility Unit*) w postaci rozproszonej sieci ze stacjami bazowymi zlokalizowanymi w Krakowie, Gdańsku, Wrocławiu, Poznaniu i na lotnisku w Kąkolewie oraz rdzeniem sieci 5GC zlokalizowanym w Poznaniu. Ponadto zastosowano również wyniesione serwery UPF (ang. *User Plane Function*) we Wrocławiu i Krakowie, aby umożliwić w tych lokalizacjach świadczenie usług na brzegu sieci. Sieć międzyregionalna jest jedną z pierwszych w Polsce prywatnych sieci 5G wykorzystujących emisje radiowe w pasmach testowych FR1 zgodnych z planem zagospodarowania częstotliwości 3.8-4.2 GHz oraz, co niewątpliwie wyróżnia infrastrukturę PL 5G, w pasmie FR2. Częstotliwości te zapewniają pokrycie sygnałem radiowym wybranych terenów ww. lokalizacji, a wspólny rdzeń sieci 5GC umożliwia realizację połączeń pomiędzy nimi.

## Laboratorium PCSS

Laboratorium 5G w Poznańskim Centrum Super-komputerowo Sieciowym (PCSS) zostało zaprojektowane dla realizacji badań funkcjonalności oraz wydajności sieci 5G, symulacji, pomiarów oraz walidacji rdzenia 5G, testowania bezpieczeństwa rdzenia 5G, udostępniania zasobów obliczeniowych i przechowywania danych, a także rozwoju aplikacji i zastosowań techniki 5G w różnych obszarach, w tym w rozwoju autonomicznych statków UAV (ang. *Unmanned Aerial Vehicle*) oraz pojazdów UGV (ang. *Unmanned Ground Vehicle*). Infrastruktura laboratorium PCSS oferuje zasoby obliczeniowe i przechowywania danych niezbędne dla realizacji eksperymentów, udostępniane przez rozproszone centrum danych. Laboratorium PCSS zostało wyposażone w system synchronizacji czasu składający się z urządzeń Oscilloquartz OSA 5412 oraz OSA 5201 zapewniających podtrzymanie synchronizacji czasu w laboratorium PL 5G na wypadek zaników sygnału GNSS lub jego zakłóceń w wyniku zagłuszania (ang. *jamming)* lub fałszowania (ang. *spoofing*). Istotnym elementem laboratorium PCSS jest AerospaceLab zlokalizowany na lotnisku w Kąkolewie. Teren lotniska jest objęty zasięgiem międzyregionalnej sieci PL 5G z 3-sektorową stacją bazową pracującej w paśmie 3,9-4,0 GHz (100 MHz), która umożliwia prowadzenie eksperymentów dotyczących rozwiązań pół-automatycznego czy autonomicznego sterowania pojazdami UAV i UGV. Ponadto AerospaceLab obejmuje również hangar zapewniający przestrzeń do lotów w warunkach kontrolowanych o wymiarach 30 m x 30 m x 10 m. Hangar ten jest objęty zasięgiem wewnątrzbudynkowej sieci 5G z dodatkową głowicą pracującą w ww. paśmie oraz z głowicą pracującą w zakresie fal milimetrowych 26 GHz (AWEUC AirScale mmWave n258 z kanałem o szerokości 100 MHz).

## Laboratorium PG

Laboratorium 5G Politechniki Gdańskiej umożliwia zarówno prowadzenie badań w środowisku ściśle kontrolowanym (przy użyciu komór i namiotów izolujących sygnały radiowe oraz unikatowego w skali projektu wielokanałowego emulatora toru radiowego MIMO 4x4), jak i realizację eksperymentów, testów i kampanii pomiarowych w terenie – włączając w to obszary miejskie o różnym przeznaczeniu, tereny niezurbanizowane, a także środowisko wód śródlądowych i akwenów morskich. Z myślą o tych ostatnich na wyposażeniu laboratorium dostępna jest flotylla dronów pływających oraz duża platforma pływająca, służąca jako baza do pomiarów na jeziorze Jelenie (w sercu Kaszub).

Poza dostępem do już wdrożonych instalacji 5G, laboratorium pozwala na tworzenie, dedykowanych do konkretnych, specyficznych badań bądź eksperymentów, heterogenicznych środowisk systemów dostępowych (zarówno 5G NR jak i non-3GPP) podłączonych do zróżnicowanego zbioru sieci rdzeniowych 5G/LTE i oferujących usługi komunikacji głosowej/wideo dla użytkowników końcowych.

Na potrzeby badań terenowych zostały przygotowane punkty instalacyjne wyposażone w zewnętrzne szafy teletechniczne, zasilanie oraz połączenia światłowodowe pozwalające na łatwe tworzenie topologii danego eksperymentu. Przygotowana infrastruktura cechuje się elastycznością i z powodzeniem może zostać wykorzystana w różnych scenariuszach przyszłych prac badawczych. Specyfika laboratorium umożliwia prowadzenie kompleksowych badań dotyczących orkiestracji zarówno elementów rdzenia sieci 5G, jak i elementów sieci dostępowych (włączając w to rozwiązania Open RAN). Badania i eksperymenty dotyczące orkiestracji elementów aplikacyjnych oraz różnorodnych aspektów przetwarzania na i poza brzegiem sieci możliwe są np. w kontekście systemów Przemysłu 4.0 (ang. *Industry 4.0*), takich jak systemy sterowania i robotyki przemysłowej oraz systemy komunikacji i automatyki morskiej.

Ważnym elementem laboratorium są też lądowe i morskie pojazdy autonomiczne i sterowane, pozwalające między innymi, na realizację badań dotyczących zastosowania tego rodzaju rozwiązań w wielu dziedzinach przemysłu oraz tworzenia i integracji systemów komunikacji o mobilnej infrastrukturze – w tym sieci pokładowych zarówno dla jednostek pływających jak i pojazdów lądowych.

Powyższą tematykę uzupełniają możliwości realizacji prac badawczych dotyczących pracy sieci w środowiskach o wysokim poziomie zakłóceń, rozwoju systemów MCPTX (ang. *Mission-critical Push-to-everything*), opracowania i weryfikacji rozwiązań nowych zaawansowanych mechanizmów lokalizacji 3D realizowanej w ramach koncepcji ISAC (ang. *Integrated Sensing & Communications*) oraz zastosowania sztucznej inteligencji w zarządzaniu

i utrzymaniu systemów komunikacyjnych oraz w aspekcie usługowym (np. elementy koncepcji Przemysłu 5.0).

## Laboratorium AGH

Laboratorium 5G w Akademii Górniczo-Hutniczej im. Stanisława Staszica w Krakowie składa się z elementów laboratorium międzyregionalnego 5G pracującego w trybie SA w oparciu o trzy sektory w paśmie 3,9 GHz oraz jeden sektor w paśmie 26 GHz na zewnątrz budynku oraz osiem sektorów w paśmie 3,9 GHz wewnątrz budynku. Lokalizacja uczelni w samym centrum miasta sprawia, że sieć AGH pokrywa swoim zasięgiem duży obszar Krakowa, w szczególności teren samej uczelni, obszar Parku Jordana, Błoń krakowskich oraz miasteczka studenckiego AGH. W celu redukcji opóźnień przekazu danych, co ma kluczowe znaczenie dla świadczenia usług czasu rzeczywistego, wykorzystano wyniesiony serwer UPF. W AGH uruchomiono również środowisko sieci 5G oparte na rozwiązaniach Open RAN, zapewniając w ten sposób większą elastyczność, interoperacyjność i innowacyjność w porównaniu do tradycyjnych, zamkniętych rozwiązań 5G. Dzięki uruchomieniu rozbudowanego środowiska radia programowalnego SDR, opartego na rozwiązaniach firmy Ettus, możliwe jest szybkie prototypowanie rozwiązań 5G przy dużej elastyczności, niskich kosztach oraz wysokiej interoperacyjności. Rozwiązania SDR stanowią fundament dla przyszłych innowacji w komunikacji bezprzewodowej, takich jak sieci 5G i 6G, umożliwiając łatwiejsze wdrażanie nowych technologii i standardów w miarę ich rozwoju. Laboratoria sieci 5G to nie tylko rozwiązania oparte na technikach 3GPP. Wdrożone rozwiązania non-3GPP oparte na standardach IEEE 802.11ax (Wi-Fi 6E) i IEEE 802.11be (Wi-Fi 7) umożliwią wykonywanie rozmaitych testów z przepływnościami sięgającymi ponad 20 Gbit/s w zakresie pasm nielicencjonowanych: 2,4 GHz, 5 GHz i 6 GHz.

Laboratorium AGH oferuje również duży klaster obliczeniowy złożony z wydajnych serwerów umożliwiających przeprowadzanie zaawansowanych badań symulacyjnych związanych z sieciami i usługami 5G. Wspomniane laboratorium jest również przystosowane do prowadzenia zaawansowanych badań w ściśle kontrolowanym środowisku radiowym. Jest ono wyposażone w programowalne tłumiki sygnału radiowego oraz matrycę przełączającą sygnały radiowe, która umożliwia podłączenie kilku niezależnych systemów 5G do komór tłumiących fale radiowe o różnych rozmiarach. Dzięki temu w komorach można w sposób zdalny badać rozmaite terminale klienckie 5G (uzyskiwane przepływności i opóźnienia transmisji, wariancję tego opóźnienia, procedury przełączania międzykomórkowego, wpływ interferencji, straty pakietów, a także zgodność z procedurami zawartymi w standardach 3GPP jak i non-3GPP). Na wyposażeniu laboratorium znajduje się również unikalny w skali projektu system monitorowania wskaźników jakości i wydajności sieci radiowych 5G o nazwie TEMS (ang. *Telecom Engineering Mobile Solutions*). To zaawansowane narzędzie do monitorowania, optymalizacji i analizy sieci komórkowych umożliwia zbieranie danych w czasie rzeczywistym oraz analizę jakości usług w sieci 5G, co obejmuje pomiar parametrów takich jak RTT (ang. *Round-Trip Time*), jitter, utracone pakiety oraz uzyskiwaną przepływność. Pozwala to na ocenę jakości usług dla różnych aplikacji i użytkowników. Dzięki analizie danych z sieci, TEMS pomaga w identyfikacji i usuwaniu problemów, takich jak zasięg, interferencje czy błędy w konfiguracji, co prowadzi do poprawy jakości świadczonych usług. TEMS umożliwia również tworzenie szczegółowych map zasięgu sieci 5G, pokazujących obszary o różnej jakości sygnału i pokrycia. Jest to szczególnie przydatne do planowania rozbudowy sieci oraz optymalizacji zasięgu. Urządzenia należące do sieci dostępowej mogą wygenerować ruch pochodzący jednocześnie od ok. 200 użytkowników końcowych.

Laboratorium AGH zostało wyposażone zarówno w autonomiczne pojazdy UAV (latające) jak i UGV (jeżdżące) mogące przenosić stosunkowo ciężki sprzęt kontrolno-pomiarowy. Dane pomiarowe w laboratorium IoT są generowane m.in. przez różnorodne czujniki środowiskowe rozlokowane na terenie uczelni. Kolejno, są one przetwarzane na brzegu sieci przez odpowiednie serwery obliczeniowe i składowane w centrum przechowywania danych. Wyposażenie laboratorium IoT zamyka platforma prototypowania rozwiązań IoT, która umożliwia budowę dowolnych urządzeń IoT z rozmaitych komponentów elektronicznych (czujniki, elementy wykonawcze, mikrokomputery i interfejsy bezprzewodowe).

Laboratorium multimedialne zostało wyposażone w przeróżne rozwiązania VR i AR umożliwiające prowadzenie wszechstronnych badań naukowych w takich dziedzinach jak: telekomunikacja, psychologia, neuronauka, edukacja, medycyna, inżynieria, sport i rehabilitacja. Zakupiony sprzęt pozwala również na prowadzenie badań społecznych i behawioralnych. Do unikalnych urządzeń znajdujących się w laboratorium multimedialnym należy system monitorowania i mapowania aktywności mózgu fNIRS (ang. *functional Near-Infrared Spectroscopy*). Główne zastosowania i funkcje fNIRS obejmują badania nad interakcją człowiek-komputer. Laboratorium wyposażono również w system skanowania przestrzeni 3D, wyświetlania treści na urządzeniach 3D, kamery nagrywające 360˚, urządzenia telekonferencji 3D, system przetwarzania obrazu z wielu kamer (8MP HDR), a także urządzenia umożliwiające realizację obiektywnej usługi pomiarowej. Całość wyposażenia laboratorium multimedialnego uzupełniają urządzenia odtwarzania dźwięku stereo oraz wielokanałowego wysokiej jakości Hi-Fi (ang. *High Fidelity*).

## Laboratorium PWr

Podstawowym celem budowy laboratoriów na Politechnice Wrocławskiej, było umożliwienie realizacji eksperymentów i prowadzenia badań na każdym z etapów projektowania, implementacji, wdrażania oraz funkcjonowania usług związanych z nowoczesnymi technikami obliczeniowymi i komunikacyjnymi.

W laboratorium są dostępne zarówno elementy laboratorium międzyregionalnego 5G, w szczególności dwie komórki pracujące w paśmie fal milimetrowych n258, jak rów-

nież sieci lokalne w pasmach 2,3 GHz oraz 3,9 GHz. Wszystkie elementy sieci radiowych są zlokalizowane są na budynkach uczelni. Infrastruktura pozwala na prowadzenie testów w warunkach rzeczywistych na obszarze między kampusem głównym a akademikami PWr. Natomiast w przypadku sieci międzyregionalnej możliwości testów terenowych rozciągają się aż do wrocławskiej siedziby IŁ-PIB. Zróżnicowana zabudowa wokół wspomnianego terenu, obejmująca zarówno obszary gęstej zabudowy, parku, domów jednorodzinnych oraz węzła wodnego rzek Odry i Oławy, pozwala na opracowanie wielu scenariuszy testów i pomiarów. Ponadto laboratorium PWr umożliwia testy technik *non–3GPP* oparte o punkty dostępowe oraz kontroler sieci 802.11 firmy Aruba.

Laboratorium PWr zostało zaprojektowane dla eksperymentów dotyczących rozproszonych systemów usługowych. Wybudowana infrastruktura pozwala na badanie rozwiązań end-to-end, uwzględniając zarówno zagadnienia komunikacyjne, jak również obliczeniowe, od poziomu warstwy fizycznej sieci dostępowej, po usługi przetwarzające dane w chmurze. Infrastruktura obliczeniowa PWr to węzeł międzyregionalnej chmury obliczeniowej. Ponadto infrastrukturę lokalną wyróżniają specjalistyczne serwery do prowadzenia obliczeń w dziedzinie uczenia maszynowego w postaci Nvidia DGX oraz do prowadzenia symulacji w środowiskach wirtualnej rzeczywistości Nvidia OVX. Wspomniany sprzęt wzbogacony został o rozwiązania programowe VMWare Horizon oraz Comtegra CGC umożliwiające wykorzystanie zasobów wielu użytkownikom jednocześnie. W szczególności możliwe jest świadczenie usług badawczych dla podmiotów, które nie posiadają wyspecjalizowanej infrastruktury, a chcą przygotować swoje rozwiązania do integracji i wdrożeń.

Wychodząc naprzeciw potrzebom badawczym w obszarze projektowania, budowania, integracji i wdrażania rozproszonych systemów usługowych, na PWr dostępne są stanowiska badawcze oraz aparatura pozwalająca na prowadzenie badań oraz prac rozwojowych m.in. w obszarze Internetu Rzeczy oraz wirtualnej i rozszerzonej rzeczywistości.

Jedno z laboratoriów badawczych to swego rodzaju Living Lab, przestrzeń, w której na co dzień pracują badacze, sama w sobie jest obiektem badań i testów w zakresie rozwiązań z obszaru inteligentnych budynków. Laboratorium jest wyposażone w stanowiska do prototypowania urządzeń IoT, drukarki i skanery 3D, osprzęt AR i VR. Ponadto dostępne są drony latające i jeżdżące, które mogą być stosowane zarówno jako źródła danych (kamery termowizyjne i multispektralne), nośniki sprzętu pomiarowego oraz baza do prototypowania złożonych rozwiązań. Część dronów komunikuje się przez wybudowane prywatne sieci 5G zarówno w zakresie przekazywania danych wizyjnych i pomiarowych, jak i sterowania. Tym samym możliwe jest budowanie kompleksowych scenariuszy obejmujących zarówno problematykę komunikacji w sieciach 5G, zdalne pilotowanie oraz systemy autonomiczne, wirtualizację i przetwarzanie dużych ilości danych, kończąc na problemach dziedzinowych systemów IoT związanych z urbanistyką, nowoczesnym rolnictwem i wielu innych obszarach. Ponadto wykorzystanie dronów pozwala na przygotowywanie bardzo dokładnych map i modeli 3D terenu, które mogą służyć zarówno celom szeroko pojętych budownictwa, architektury i urbanistyki, ale również jako baza dla problemów planowania radiowego, symulacji propagacji, czy innym scenariuszom symulacyjnym.

## Laboratorium IŁ-PIB

Laboratorium Instytutu Łączności - Państwowego Instytutu Badawczego jest ukierunkowane głównie na badania i pomiary w najniższych warstwach sieci 5G (fizycznej PHY, łącza danych MAC) oraz na aplikacjach wykorzystywanych w sieci 5G. Realizowane w nim są również badania zgodności z odpowiednimi normami dotyczącymi kompatybilności elektromagnetycznej a także zgodności parametrów radiowych. W IŁ-PIB we Wrocławiu wybudowano w tym celu w ramach projektu budynek laboratoryjny, w którym umieszczono zaprojektowaną specjalnie do celów projektu komorę bezodbiciową hybrydową składającą się z komory SAC 10M (ang. *semi-anechoic chamber*) o odległości pomiarowej 10 m oraz FAR 3M (ang. *full anechoic room*) o odległości pomiarowej 3 m, a także zintegrowanego systemu do pomiarów anten w strefie bliskiej realizowanych w komorze. Laboratorium jest wyposażone również w szereg przyrządów pomiarowych wspierających badania w najniższych warstwach, tj. analizator widma, oscyloskop, odbiornik pomiarowy do pomiarów kompatybilności elektromagnetycznej EMC a także urządzenia i oprogramowanie do badań zasięgów sieci 5G i pomiarów w ruchu (drive-testy) i badań propagacji fal radiowych. Laboratorium IŁ-PIB umożliwia również prace z wykorzystaniem nowych technik radiowych (np. emisje nieortogonalne) a także projektowanie sieci radiowych 5G z wykorzystaniem profesjonalnego oprogramowania planistycznego.

## Laboratorium PW

Laboratorium Politechniki Warszawskiej jest ukierunkowane na prowadzenie eksperymentów w czterech głównych obszarach obejmujących: 1) badania sieci dostępu radiowego 5G NR, Open RAN, zbudowanych na urządzeniach pochodzących od różnych producentów w ściśle kontrolowanym środowisku radiowym oraz ich współpracy z rdzeniem sieci 5G oraz technikami obliczeń na brzegu sieci (ang. *edge computing*), 2) rozwój funkcjonalności rdzenia sieci 5G oraz metod orkiestracji i zarządzania konteneryzowanymi funkcjami rdzenia CNF (ang. *Cloud Native Functions*) wdrożonych w zintegrowanej infrastrukturze sieciowo-obliczeniowej ECC (ang. *Edge-Cloud Continuum*) utworzonej z heterogenicznych, rozproszonych klastrów obliczeniowych pochodzących od różnych dostawców, 3) badania technik wirtualizacji i sieci programowalnych, w tym wykorzystujących język P4, 4) zastosowania techniki 5G dla tworzenia i wykorzystania cyfrowych modeli rzeczywistości, obejmujące odwzorowanie obiektów rzeczywistych do postaci cyfrowej, prezentacje obrazów wirtualnej, rozszerzonej i mieszanej

rzeczywistości (VR/AR/MR) oraz przetwarzanie i strumieniowanie immersyjnych obrazów wideo o wysokiej jakości.

Szczególnie istotnym elementem wyposażenia laboratorium PW jest kontrolowane środowisko radiowe zbudowane na bazie 256-kanałowej, programowalnej matrycy przełączającej sygnały radiowe, wyposażonej w programowalne tłumiki sygnału radiowego. Matryca ta umożliwia dołączenie sygnału radiowego generowanego z głowic stacji bazowych 5G i emulatorów użytkowników do zestawu 6 komór izolujących sygnały radiowe, które są wyposażone w systemy antenowe, w tym systemy MIMO 4x4. W komorach umieszczono terminale sieci 5G (smartfony 5G, modemy 5G) oraz terminale IoT, do których dostęp uzyskano za pomocą zdalnego pulpitu. Matryca umożliwia zdalną rekonfiguracje torów radiowych oraz programowanie zmieniającego się w czasie tłumienia w poszczególnych torach radiowych. Utworzone kontrolowane środowisko radiowe umożliwia realizację powtarzalnych eksperymentów dla dowolnego zakresu częstotliwości, konfiguracji kanałów radiowych i systemów antenowych, trybów transmisji wspieranych przez stacje bazowe i terminale. Badania dotyczą m.in. wydajności transmisji radiowej systemów 5G (przepływności bitowej, zasięgu, poziomu sygnału), badanie procedur przełączania (ang. *handover*), transmisji MIMO, wpływu interferencji, współpracy elementów sieci RAN pochodzących od różnych producentów, w tym kompatybilności terminali oraz współpracy z systemami non 3GPP.

W obszarze badań otoczenia sieci 5G istotnym wyposażeniem laboratorium jest stanowisko cyfrowego modelowania rzeczywistości, które umożliwia skanowanie obiektów 3D, tworzenie ich modeli i odwzorowania w cyfrowym świecie, a następnie ich przetwarzania i strumieniowania w postaci obrazów immersyjnych o wysokiej jakości, z wykorzystaniem techniki 5G i obliczeń na brzegu sieci i prezentacji na okularach rozszerzonej lub mieszanej rzeczywistości.

## OBSZARY BADAŃ 5G/6G

Infrastruktura PL 5G oferuje szeroki zakres usług badawczych dotyczących zarówno rozwoju techniki 5G/6G, jak również rozwoju potencjalnych jej zastosowań, a także testowania wdrażanych rozwiązań. Istotną cechą infrastruktury PL 5G jest oferowanie najnowszych rozwiązań 5G pochodzących od wiodących producentów, zapewnienie dostępu do specjalizowanych urządzeń pomiarowych przeznaczonych do badania transmisji radiowej, walidacji i badania wydajności elementów sieci 5G oraz analizy podatności i bezpieczeństwa sieci 5G, oraz wsparcie wysoko wykwalifikowanej kadry z wiodących krajowych ośrodków badawczych. Poniżej scharakteryzowano wybrane obszary badań dotyczących systemów 5G, które są przewidziane w infrastrukturze PL 5G:

- **Badania w obszarze radiowych sieci dostępowych,** dotyczą m.in. 1) możliwości współpracy sprzętu 5G pochodzącego od różnych producentów, 2) efektywności przekazu danych w systemach 5G wykorzystujących systemy wieloantenowe (ang. *massive MIMO*), metod formowania wiązki i transmisji w zakresie fal milimetrowych, 3) protokołów dostępowych i metod sterowania wykorzystujących skorelowaną, jednoczesną transmisję, 4) metod sterowania i zarządzania zasobami radiowymi, w tym wykorzystujące metody uczenia maszynowego, 5) bezpieczeństwa radiowej sieci dostępowej i identyfikacji podatności dostępnych rozwiązań, 6) współpracy pomiędzy wydzielonymi sieciami RAN, a także 7) współpracy i współistnienia komercyjnych, prywatnych oraz militarnych systemów 5G, i 8) nowych technik radiowych w przyszłych systemach radiowych (np. techniki nieortogonalne).
- **Rozwój rozwiązań typu Open RAN** [7], ich potencjału oraz zagrożeń. W szczególności laboratorium PL 5G oferuje platformę Open RAN firmy Radisys, która umożliwia tworzenie aplikacji sterujących siecią RAN w ramach tzw. inteligentnych sterowników RIC (ang. *RAN Inteligent Controller*). Platforma ta jest zgodna z zaleceniami stowarzyszenia O-RAN Alliance i zapewnia otwarte interfejsy programistyczne, co umożliwia opracowanie własnych aplikacji xApps / rApps, sterujących działaniem sieci RAN. Platforma ta może zostać również wykorzystana do badań dotyczących bezpieczeństwa systemów O-RAN. W szczególności, zgodnie z zaleceniami grupy WG11, badania dotyczące bezpieczeństwa O-RAN obejmują bezpieczeństwo O-Cloud, bezpieczeństwo zarządzania usługami i orkiestracji, bezpieczeństwo współdzielonego O-RU oraz bezpieczeństwo Near Real-Time RIC i xApps.
- **Badania w obszarze rdzenia sieci 5G** dotyczą m.in. 1) współpracy autonomicznych sieci 5G, 2) metod orkiestracji i zarządzania usługami 5G w modelu CNF, w tym skalowania wydajności, zapewnienia niezawodności w warunkach dynamicznych zmian topologii i niedostępności zasobów infrastruktury, 3) identyfikacji podatności i zapewnienia bezpieczeństwa rdzenia sieci 5G, 4) interoperacyjności i współpracy z systemami łączności niezgodnymi ze standardem 5G, np. WiFi, sieci radiowe, 5) wsparcia mobilności użytkowników, infrastruktury systemu 5G (sieci RAN, elementów rdzenia 5G) a także oferowanych usług.
- **Badanie możliwości utworzenia i współpracy wydzielonych sieci do zastosowań specjalnych,** np. wojskowych (ang. *military slice*) w ramach infrastruktury komercyjnych i prywatnych sieci 5G. Laboratorium PL 5G umożliwia utworzenie i udostępnienie wydzielonych sieci (ang. *network slices*) w ramach infrastruktury sieci międzyregionalnej bazującej na rozwiązaniu komercyjnym firmy NOKIA oraz na podstawie rozwiązania Open5GCore firmy Fraunhofer.
- **Badania narzędzi wirtualizacyjnych** bazujących na maszynach wirtualnych i kontenerach, a także środowisk wirtualizacyjnych stanowiących podstawę dla wdrożenia systemów 5G w postaci wirtualnych funkcji sieciowych. W szczególności badania te dotyczą wykorzystania akceleratorów sprzętowych i metod uczenia maszynowego.
- **Badania dotyczące techniki przetwarzania na brzegu sieci MEC** (ang. *Multiaccess Edge Computing*) i przyszłych rozwiązań zintegrowanej infrastruktury sieciowo-obliczeniowej ECC (ang. *Edge-Cloud Continuum*) [8] bazujących na zasobach obliczeniowych pochodzących do wielu

dostawców. W rozwiązaniach militarnych szczególnie istotnym elementem jest wykorzystanie zasobów różnych rodzajów wojsk, oddziałów dostępnych w danym scenariuszu operacyjnym.

- **Badania metod samoorganizacji sieci 5G i metod zarządzania siecią i usługami bazujących na paradygmacie ZSM (ang. *Zero touch network & Service Management)***, które umożliwiają autokonfigurację systemu i automatyczną rekonfigurację i adaptację systemu 5G w zależności od aktualnie dostępnych zasobów i środków łączności. Zarządzanie ZSM to ewoluująca koncepcja prowadzona z inicjatywy ETSI [9], której celem jest zapewnienie środowiska w pełni zautomatyzowanej oraz samozarządzalnej sieci 5G. Ideą ZSM jest wprowadzenie w sieciach technik umożliwiających dokonywanie samodzielnej konfiguracji bez konieczności bezpośredniej interwencji człowieka. Celami ZSM są: autonomiczna zmiana konfiguracji umożliwiająca samodzielną optymalizację w celu lepszego dostosowania do panującej sytuacji, samodzielna naprawa w celu zapewnienia prawidłowego funkcjonowania, samodzielne monitorowanie w celu śledzenia jego funkcjonowania i samodzielne skalowanie w celu dynamicznego angażowania lub odłączania zasobów w zależności od bieżących potrzeb.
- **Badania kompatybilności elektromagnetycznej i badań systemów antenowych (SAC i FAR)** w komorze hybrydowej SAC 10M i FAR 3M zlokalizowanej w Instytucie Łączności - PIB we Wrocławiu. W komorze będą mogły być wykonywane pomiary kompatybilności elektromagnetycznej, zakłóceń międzysystemowych, odporności i emisyjności urządzeń, a także badań charakterystyk systemów antenowych 5G czy parametrów urządzeń 5G (np. TRP, EIRP czy pomiary czułości urządzeń, badania współczynników ochronnych czy selektywności) oraz badania zgodności urządzeń z odpowiednimi normami (m.in. ETSI, 3GPP).
- **Badania możliwości wykorzystania sieci 5G w środowisku morskim** oraz badań dotyczących nowych rozwiązań i aplikacji dla bezzałogowych pojazdów powietrznych oraz naziemnych (lotnisko w Kąkolewie) oraz zastosowania w środowisku miejskim (Gdańsk/Kraków/Wrocław).
- **Badanie systemów kwantowej dystrybucji kluczy QKD (ang. *Quantum Key Distribution*) w systemach 5G**. W trwającej obecnie rozbudowie laboratorium PL 5G utworzone zostaną nowe stanowiska badawcze dotyczące kwantowej dystrybucji kluczy QKD na duże odległości (łącze QKD Poznań-Warszawa) i ich integracja z systemami 5G.
- **Badania wykorzystania możliwości i potencjału zastosowań technologii wirtualnej, rozszerzonej oraz mieszanej rzeczywistości** w kontekście tworzenia innowacyjnych aplikacji, które mogą zostać dostosowane do potrzeb poszczególnych gałęzi zastosowań, takich jak przemysł, wojsko, służby mundurowe czy edukacja. Należy podkreślić, że technologie VR/AR/MR umożliwiają użytkownikom wejście w wirtualny świat, zapewniając interakcję zarówno z wirtualnymi, jak i realnymi elementami otaczającego świata.
- **Badania w obszarze bezpieczeństwa** dotyczą wymienionych powyżej obszarów. W szczególności: 1) analizy bezpieczeństwa zwirtualizowanej infrastruktury sieci 5G i identyfikacji potencjalnych podatności, 2) bezpieczeństwa sieci Open RAN, 3) bezpieczeństwa przetwarzania danych z wykorzystaniem sztucznej inteligencji oraz uczenia maszynowego, 4) bezpieczeństwa wykorzystania technologii network slicing w zastosowaniach specjalnych, 5) bezpieczeństwa w sieciach ZSM.
- **Badania w obszarze dziedzinowych systemów usługowych**, które z jednej strony korzystają z nowoczesnych technik komunikacyjnych takich jak 5G/6G, a jednocześnie wymagają infrastruktury obliczeniowej. Naturalnym krokiem w rozwoju systemów usługowych w wielu dziedzinach jest wykorzystanie metod uczenia maszynowego i szeroko rozumianej sztucznej inteligencji. Tego typu systemy wymagają niezawodnych, szeroko dostępnych technik komunikacji o niskich opóźnieniach oraz coraz większej przepustowości między urządzeniami końcowymi z zasobami obliczeniowymi w chmurze lub na brzegu sieci.
- **Badania w obszarze sterowania dronami, wodnymi, lądowymi i powietrznymi**. Nieodłącznymi scenariuszami wskazywanymi przy omawianiu technik komunikacji takich jak 5G jest problematyka sterowania statkami bezzałogowymi, zarówno w kontekście wykonywania misji ręcznie jak i wsparcia misji autonomicznych. Tematyka tych badań obejmuje zarówno kwestie komunikacji, takie jak planowanie radiowe na wysokościach lotu dronów oraz zapewnienie pewnej komunikacji przy utracie łączności podstawowej, jak również kwestie związane z przetwarzaniem pozyskiwanych w ramach misji danych.

## PRZYKŁADOWE EKSPERYMENTY

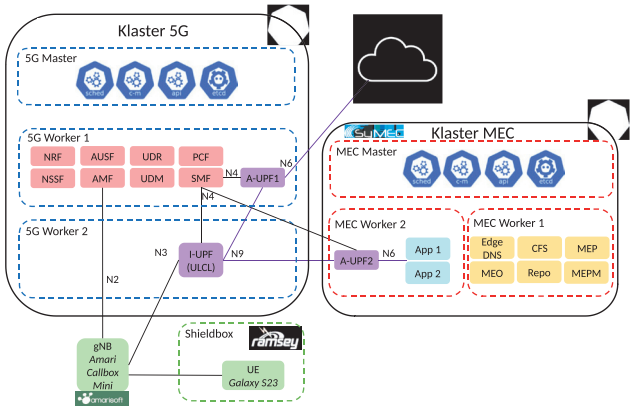
Przedstawiamy przykładowe eksperymenty przeprowadzone z wykorzystaniem infrastruktury PL 5G.

### Eksperyment dotyczący orkiestracji w środowisku ECC

Jednym z wyzwań dotyczących rozwoju techniki 6G jest opracowanie efektywnych algorytmów orkiestracji w zintegrowanej infrastrukturze sieciowo-obliczeniowej ECC. Celem tych algorytmów jest zarządzanie rozmieszczeniem i liczbą uruchamianych instancji elementów danego systemu, np. funkcji sieciowych w przypadku rdzenia sieci 5/6G lub aplikacji w przypadku Systemu MEC (System MEC służy do uruchamiania aplikacji w bliskiej odległości do użytkowników końcowych, np. przy stacjach bazowych, co pozwala na lokalne przetwarzanie danych i obsługę żądań, tym samym zmniejszając opóźnienie w relacji koniec-koniec oraz obciążenie sieci [10]). W szczególności jest niezbędne opracowanie orkiestratora, który zarządza jednocześnie wieloma tego typu systemami, umożliwiając optymalne rozmieszczenie ich poszczególnych elementów.

W rozważanym eksperymencie analizowane są algorytmy orkiestrujące instancjami funkcji UPF oraz aplikacji MEC na wspólnych zasobach, uwzględniając możliwości obsługowe / chwilowe zapotrzebowanie obydwu z nich: więcej

aplikacji MEC uruchomionych w danym miejscu skutkuje większą ilością ruchu do niego przesyłanego, co może doprowadzić do przeciążenia funkcji UPF i degradacji usługi; natomiast znaczne przewymiarowanie UPF zabiera zasoby, które mogłyby być użyte przez aplikacje MEC. Przykładowe środowisko do tego typu badań przedstawia *rJest ono zbudowane z dwóch klastrów Kubernetes („Klaster 5G" oraz „Klaster MEC"), stacji bazowej oraz telefonu umieszczonego w komorze izolującej sygnały radiowe. W Klastrze 5G znajduje się funkcja I-UPF (ULCL), tj. Uplink Classifier, która decyduje, do której instancji UPF powinien zostać przekierowany dany ruch (bazując np. na docelowym adresie IP, nazwie domenowej, itp.). Domyślnym wyjściem z sieci rdzeniowej jest UPF oznaczony jako A-UPF1 znajdujący się w Klastrze 5G, natomiast ruch przeznaczony dla aplikacji MEC będzie kierowany do obsługi w UPF uruchomionym w Klastrze MEC (A-UPF2). Tym samym A-UPF2 obsługuje wyłącznie ruch przeznaczony dla aplikacji MEC znajdujących się w tym samym klastrze, w którym sam jest uruchomiony. Trasę pakietów do poszczególnych aplikacji (znajdujących się w Internecie / w Systemie MEC) można śledzić bezpośrednio z poziomu telefonu, do którego zapewniony jest zdalny pulpit.*

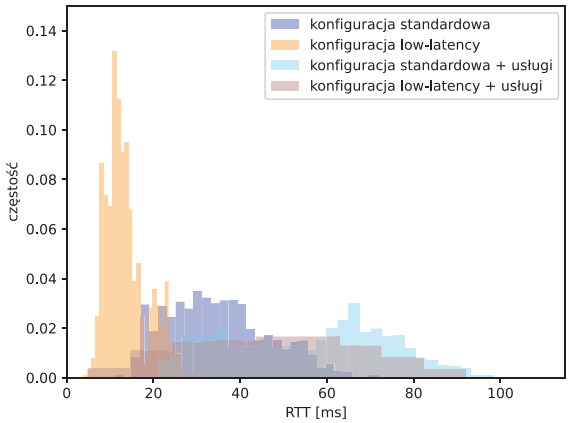



» *Rys. 2. Przykład wdrożenia sieci 5G w dwuklastrowym środowisku ECC*
» *Fig. 2. Exemplary 5G deployment in Edge Cloud Continuum environment*

Jest ono zbudowane z dwóch klastrów Kubernetes („Klaster 5G" oraz „Klaster MEC"), stacji bazowej oraz telefonu umieszczonego w komorze izolującej sygnały radiowe. W Klastrze 5G znajduje się funkcja I-UPF (ULCL), tj. *Uplink Classifier*, która decyduje, do której instancji UPF powinien zostać przekierowany dany ruch (bazując np. na docelowym adresie IP, nazwie domenowej, itp.). Domyślnym wyjściem z sieci rdzeniowej jest UPF oznaczony jako A-UPF1 znajdujący się w Klastrze 5G, natomiast ruch przeznaczony dla aplikacji MEC będzie kierowany do obsługi w UPF uruchomionym w Klastrze MEC (A-UPF2). Tym samym A-UPF2 obsługuje wyłącznie ruch przeznaczony dla aplikacji MEC znajdujących się w tym samym klastrze, w którym sam jest uruchomiony. Trasę pakietów do poszczególnych aplikacji (znajdujących się w Internecie/w Systemie MEC) można śledzić bezpośrednio z poziomu telefonu, do którego zapewniony jest zdalny pulpit.

## Analiza opóźnień na potrzeby rozwiązań Przemysłu 4.0

Jedną z istotnych i oczekiwanych usług oferowanych w systemach 5G jest usługa URLLC zapewniająca możliwości niezawodnej komunikacji z niewielkim opóźnieniem. Niestety pomimo dużego zapotrzebowania na tego typu łączność, w chwili obecnej, na rynku komercyjnym nie są dostępne terminale końcowe pozwalające na realizację takich scenariuszy. Nie wstrzymuje to jednak intensywnie prowadzonych obecnie prac badawczych ukierunkowanych na wykorzystanie rozwiązań 5G NR na potrzeby instalacji systemów Przemysłu 4.0.




» *Rys. 3. Histogram wartości opóźnienia RTT dla analizowanych scenariuszy w przykładowym eksperymencie oceny stosowalności rozwiązań 5G NR na potrzeby komunikacji w systemach Przemysłu 4.0*
» *Fig. 3. Exemplary RTT histogram measured to evaluate the applicability of 5G NR solutions for communication in Industry 4.0 systems*

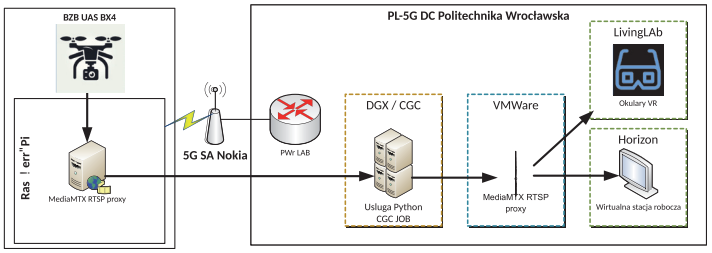
W związku z wspomnianymi ograniczeniami istotna staje się ocena wartości parametrów komunikacji (głównie opóźnienia) możliwych do uzyskania przy wykorzystaniu dostępnych obecnie systemów 5G oraz działania mające na celu ich poprawę, dzięki odpowiedniej konfiguracji parametrów stacji gNB i rdzenia sieci. Na potrzeby realizacji tego typu prac, w ramach Laboratorium 5G Politechniki Gdańskiej, wykorzystywana jest stacja bazowa Amarisoft Callbox Classic pracująca w paśmie 3,95 GHz w konfiguracji MIMO 2x2 i szerokości kanału 40 MHz. Elementem systemu Przemysłu 4.0 podłączonym do, tak utworzonej, prywatnej sieci 5G jest mobilna platforma kołowa Husarion Panther wyposażona w czujniki wizyjne w postaci kamery przemysłowej Milesight MS-C2971-X23RPE, LIDARu Outer OS0-128U i modułu komunikacyjnego Siemens SCALANCE MUM853-1. Na platformie mobilnej uruchomione zostały usługi przesyłania obrazu z kamery oraz danych z czujnika LIDAR do serwera brzegowego, na którym realizowane są wizualizacja oraz analiza danych. Na otrzymane wyniki wskazują, że odpowiednie przygotowanie konfiguracji systemu 5G pozwala znacząco zredukować czas wymiany wiadomości sterowania platformą mobilną. Zaprojektowane i zbudowane stanowisko wykorzystywane jest do dalszych prac w tym zakresie. przedstawiono przykładowe zestawienie wartości opóźnienia RTT (ang. *Round Trip Time*) prezentujących wyniki uzyskane dla domyślnej kon-

figuracji stacji bazowej zaproponowanej przez producenta oraz po zastosowaniu konfiguracji pozwalającej na zmniejszenie opóźnienia.

Otrzymane wyniki wskazują, że odpowiednie przygotowanie konfiguracji systemu 5G pozwala znacząco zredukować czas wymiany wiadomości sterowania platformą mobilną. Zaprojektowane i zbudowane stanowisko wykorzystywane jest do dalszych prac w tym zakresie.

## Eksperyment z wykorzystaniem drona i zasobów GPU

Jak wcześniej wspomniano infrastruktura PL 5G obejmuje nie tylko obszar sieci 5G, ale również szeroko rozumianego otoczenia. Jednym z przykładowych scenariuszy wiążących wiele elementów wyposażenia, w tym przypadku PWr jest scenariusz przetwarzania obrazu pozyskiwanego w czasie zbliżonym do rzeczywistego z bezzałogowego statku powietrznego.




» *Rys. 4. Scenariusz usługi analizy obrazów wideo*
» *Fig. 4. Video analytics service scenario*

Drony firmy BZB UAS wyposażone w komputery jednopłytkowe oraz modemy 5G umożliwiają bezpośrednią transmisję z kamer (wideo, IR oraz multispektralnej) z wykorzystaniem protokołu RTSP. Do komunikacji wykorzystywana jest sieć międzyregionalna 5G. Na tym etapie możliwe jest monitorowanie parametrów połączenia m.in. na stacji bazowej poprzez analizę liczników jak również poprzez pozyskanie zrzutów ruchu pomiędzy elementami rdzenia, dla lepszego zrozumienia problemów np. podczas przełączeń między stacjami.

Strumień multimedialny jest przekazywany dalej do środowiska obliczeniowego, gdzie mogą być uruchamiane usługi takie jak wykrywanie obiektów w obrazie. Kolejnym etapem jest wykorzystanie międzyregionalnego zasobu obliczeniowego w postaci maszyny wirtualnej, gdzie uruchomiony jest multimedialny serwer proxy. Takie podejście umożliwia rozdzielenie strumienia i jego wykorzystanie w innych eksperymentach.

## PODSUMOWANIE

W artykule przedstawiono infrastrukturę Krajowego laboratorium sieci i usług 5G (PL 5G), które zostało utworzone dla realizacji praktycznych badań dotyczących rozwoju techniki 5G oraz przyszłych generacji systemów komunikacji mobilnej tj. 6G. W szczególności omówiono architekturę laboratorium obejmującą ogólnopolską sieć międzyregionalną oraz lokalne sieci prywatne, wyposażenie laboratorium a także przykładowe eksperymenty przeprowadzone w jego wykorzystaniem. Ponadto w artykule przedstawiono zarys tematyki badań dotyczących rozwoju systemów 5G i 6G, które mogę być prowadzone z wykorzystaniem infrastruktury PL 5G, Przedstawiony zarys eksperymentów nie wyczerpuje pełnego spektrum możliwości zastosowania infrastruktury PL 5G. Należy podkreślić, iż laboratorium jest otwarte dla realizacji eksperymentów zarówno przez jednostki badawcze jak i podmioty komercyjne a także jednostki potencjalnie zainteresowane wdrożenie techniki 5G w różnych obszarach działalności. Dostęp do laboratorium i realizacja eksperymentów może być prowadzona w sposób zdalny z wykorzystaniem strony internetowej portal.pl5g.pl. Zasady dostępu, regulaminy korzystania i cenniki są również dostępne na wspomnianym portalu.

*Prace, których wyniki są przedstawione w tym artykule, były prowadzone w ramach projektu POIR.04.02.00-00-D008/20, pt. „Krajowe laboratorium sieci i usług 5G wraz z otoczeniem", współfinasowanego w ramach Programu Operacyjnego Inteligentny Rozwój na lata 2014-2020.*

## LITERATURA

[1] J. Woźniak (ed), „Tendencje w rozwoju polskiej i światowej telekomunikacji i teleinformatyki", Wojskowa Akademia Techniczna, 2020, isbn: 978-83-7938-292-7
[2] T. Taleb et al, „White Paper on 6G Networking. 6G Research Visions", No. 6, University of Oulu, 2020 http://urn.fi/urn:isbn:9789526226842
[3] Ö. Bulakçı et al, "Towards Sustainable and Trustworthy 6G: Challenges, Enablers, and Architectural Design", Boston-Delft, 2023, http://dx.doi.org/10.1561/9781638282396 (dostęp 1.07.2024)
[4] SK Telecom, "6G White Paper: 5G Lessons Learned, 6G Key Requirements, 6G Network Evolution, and 6G Spectrum", SK Telecom, 2023 https://bit.ly/4a27B9I , dostęp 1.07.2024,
[5] Inicjatywa SLICES, https://www.slices-ri.eu/ (dostęp 1.07.2024)
[6] W. Burakowski et al, "Planowane krajowe laboratorium badawcze sieci i usług 5G wraz z otoczeniem", Przegląd telekomunikacyjny - wiadomości telekomunikacyjne, nr 9, 2022, strony 110-115, DOI:10.15199/59.2022.4.3.
[7] M. Poles, L. Bonati, S. B. Salvatore D'Oro, T. Melodia, „Understanding O-RAN: Architecture, Interfaces, Algorithms, Security, and Research Challenges" CoRR, 2022, https://arxiv.org/abs/2202.01032
[8] B.M. Khorsandi, M. Hoffmann, M. Uusitalo, M-H. Hamon, B. Richerzhagen, G. D'Aria, A. Gati, D. Lopez (ed), "Deliverable D1.3: Targets and requirements for 6G – initial E2E architecture", Hexa-X project, 2022, https://hexa-x.eu/wp-content/uploads/2022/03/Hexa-X_D1.3.pdf (dostęp 1.07.2024)
[9] "Zero-touch network and service management (ZSM); terminology for concepts in ZSM," Sierpień 2023, https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/007/02.01.01_60/gs_ZSM007v020101p.pdf (dostęp 1.07.2024)
[10] A. Bęben, et al, "Implementacja architektury systemu SyMEC", Przegląd Telekomunikacyjny – wiadomości telekomunikacyjne, no 4, 2022, strony 315-320.

DOI: 10.15199/59.2024.4.5

# Recent Advances in Open RAN Systems

## Aktualny stan standaryzacji systemów otwartych sieci dostępowych (Open RAN)

dr inż. MARCIN DRYJAŃSKI
Rimedo Labs
marcin.dryjanski@rimedolabs.com

ABSTRACT Since its establishment in 2020, the O-RAN ALLIANCE has undergone significant updates to the specifications of O-RAN. There have been notable advancements in the architectural aspects, interface details, and function definitions. The working groups release technical documents apaproximately every six months, new focus groups are formed, and emerging topics of interest are addressed. In line with the research advancements towards 6G in the field, the O-RAN ALLIANCE also considers this aspect. Recent trends such as security and energy efficiency in mobile networks are also being incorporated. This article provides an overview of the current status of standardization efforts and highlights the ongoing focus of the O-RAN ecosystem as per the abovementioned aspects.
KEYWORDS Open Radio Access Networks, O-RAN, 5G, Network Intelligence

STRESZCZENIE Od momentu swojego powstania w 2020 roku, O-RAN ALLIANCE dokonała znacznych aktualizacji specyfikacji otwartych radiowych sieci dostępowych (Open RAN). Doszło do znaczących postępów w zakresie aspektów architektonicznych, szczegółów interfejsu i definicji funkcji. Grupy robocze wydają dokumenty techniczne mniej więcej co sześć miesięcy, tworzone są nowe grupy robocze, a adresowane są również nowe interesujące tematy. Wraz z postępami badań w kierunku 6G, O-RAN ALLIANCE bierze je również pod uwagę. Uwzględniane są także ostatnie trendy, takie jak bezpieczeństwo i efektywność energetyczna w sieciach mobilnych. W niniejszym artykule przedstawiono przegląd bieżącego stanu prac standaryzacyjnych i wyeksponowano bieżące tematy opracowywane w ekosystemie O-RAN zgodnie z nimi.
SŁOWA KLUCZOWE Otwarte dostępowe sieci radiowe, O-RAN, 5G, inteligencja sieci

Openness, flexibility, and disaggregation are the guiding principles for the next generation of wireless communication networks. Unlike the conventional radio access network (RAN) design, where a single vendor supplies most RAN elements in a closed system, the Open RAN concept involves multiple vendors providing specialized RAN modules. This modular approach allows operators to update and improve specific network functionalities without replacing the entire system. Operators have control over which functions to activate, deactivate, enhance, maintain, or remove. These adjustments can be made through software module manipulation, enabling continuous integration and continuous development (CI/CD) for incremental system improvements.

Traditionally, the radio access network (RAN) is provided as a single, closed system managed by one vendor, with internal interfaces that are not accessible to others. Transitioning to Open RAN involves dividing the base station (BS) functions into separate entities — a centralized unit (CU), a distributed unit (DU), and a remote unit (RU) — with open interfaces connecting them. This allows different vendors to develop these entities independently, facilitated by open interfaces like Open Fronthaul (Open FH). Another key component is the RAN intelligent controller (RIC), which is separated from the processing units and provides management functions such as radio resource management (RRM) and self-organizing networks (SON). In the Open RAN model, intelligence is integrated into the system via artificial intelligence (AI) models for radio network automation.

Summarizing, the O-RAN concept is characterized by:

- Disaggregation of the RAN into CU, DU, RU, and RIC functions, separating software from hardware (virtualization) and opening internal RAN interfaces.
- Creation of an open ecosystem where different vendors, such as CU/DU vendors, RIC vendors, xApp developers, and system integrators, can collaborate.
- Intelligent management enabled by the RIC, embedding AI models and specialized RRM functions like Traffic Steering, Mobility Management, and Interference Management within the O-RAN architecture.

The O-RAN ALLIANCE [1] spearheads the standardization of Open RAN, advocating for an open and modular RAN architecture. Their released standards outline the overall

Open RAN architecture, requirements, and functionalities. Importantly, new open interfaces have been introduced to motivate xApp/rApp providers to develop and deliver new algorithms for various aspects of wireless communications.

The article is composed of three main parts. In Section 2, the O-RAN architecture is presented, focusing on the new elements of the RAN compared to the traditional approaches. In Section 3, the focus is on the current standardization activities, while in Section 4, the key topics within the O-RAN ecosystem are elaborated. Finally, Section 5 captures the conclusions from the discussion.

## O-RAN ARCHITECTURE

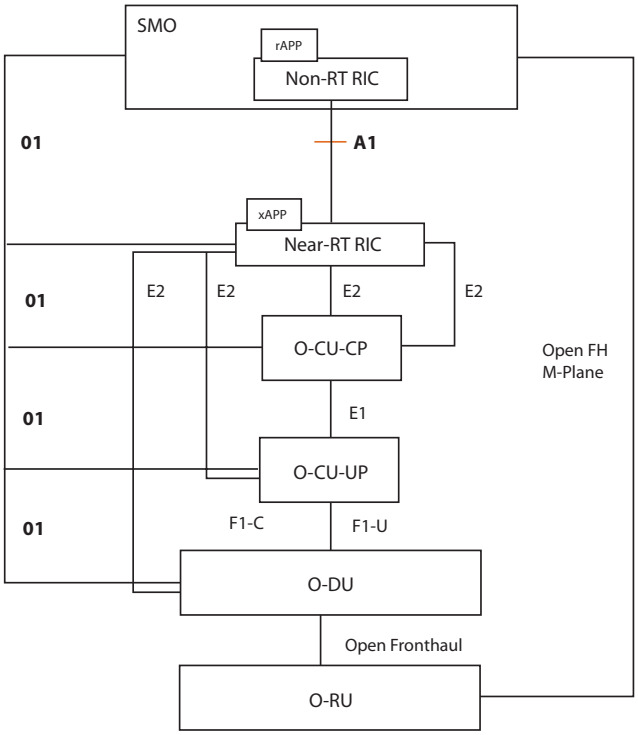
The O-RAN architecture is shown in *Fig. 1* [2]. In 5G, the centralized unit (CU) is further divided into two entities: CU-CP (Control Plane for connection management) and CU-UP (User Plane for data processing). Additionally, unlike LTE, the user plane (UP) includes the Service Data Adaptation Protocol (SDAP) protocol for quality of service (QoS) mapping. In the O-RAN architecture, these components are prefixed with "O-" (e.g., O-CU-UP, O-CU-CP, O-DU, O-RU) to denote their adaptation to the O-RAN ALLIANCE standards. These components are connected via the E2 interface and are referred to as E2 nodes in O-RAN specifications.

On the other side of the E2 interface is the RAN Intelligent Controller (RIC), which is divided into "Near-Real Time RIC" (Near-RT RIC) and "Non-Real Time RIC" (Non-RT RIC), potentially provided by third parties. The Near-RT RIC manages near-real-time radio resource management functions (ranging from >10 ms to <1 s), such as Mobility Management and Interference Management. The Non-RT RIC handles higher-level functions and provides policies to the Near-RT RIC via the A1 interface. It is important to note that real-time (RT) radio resource management (RRM) remains embedded within the O-DU, handling tasks like MAC scheduling and power control.

To summarize, there are three control loops in this hierarchical design: RT (<10 ms) managed by the O-DU, near-RT (>10 ms to <1 s) managed by the Near-RT RIC, and Non-RT (>1 s) managed by the Non-RT RIC. This hierarchical structure allows for the separation of resource management tasks based on their time scales.

Here are the details of the individual building blocks in the O-RAN architecture [2]:

- O-CU-CP: This logical node hosts the Radio Resource Control protocol (RRC) and the control plane part of the Packet Data Convergence Protocol (PDCP). It terminates the F1-C, E1, E2, O1, X2/Xn-C, and NG-C interfaces. It is referred to as an E2 Node due to its connection to the RIC via the E2 interface.
- O-CU-UP: This logical node hosts the SDAP and the user plane part of PDCP. It terminates the F1-U, E1, E2, O1, X2/Xn-U, and NG-U interfaces and is also referred to as an E2 Node.




» *Fig. 1. O-RAN architecture*
» *Rys. 1. Architektura systemu O-RAN*

- O-DU: This logical node hosts the Radio Link Control (RLC), Medium Access Control (MAC), and the upper part of the physical layer (High-PHY) protocols. It terminates the F1, E1, E2, O1, and Open Fronthaul (O-FH) interfaces, and is also known as an E2 Node.
- O-RU: This physical node hosts the lower part of the physical layer (Low-PHY) protocol and terminates the O-FH and O-FH M-Plane interfaces.
- Service Management and Orchestration (SMO): This subsystem is responsible for RAN management, including the Non-RT RIC for RAN optimization, cloud platform management, and terminating the Fault, Configuration, Accounting, Performance, Security (FCAPS) interface towards O-RAN network functions.
- Near-RT RIC: This logical function enables near real-time control and optimization of E2 Node functions and resources using data collection and actions over the E2 interface with control loops in the range of tens of milliseconds. It hosts one or more xApps providing value-added services (VAS) through RRM/SON algorithms and terminates the E2, A1, and O1 interfaces.
- Non-RT RIC: Within the SMO, this logical function supports intelligent RAN optimization by providing policy-based guidance, ML model management, and enrichment information (EI) to the Near-RT RIC through the A1 interface. It hosts one or more rApps offering VAS via optimization algorithms, primarily AI/ML-based, and terminates the A1 interface.

- xApp: A modular application running on the Near-RT RIC, independent of it and potentially provided by third parties. xApps are associated with specific RAN functionalities in the E2 Node through the E2 interface, offering services such as load balancing, handover optimization, interference management, and slice control.
- rApp: A modular application leveraging the Non-RT RIC framework to provide VAS related to RAN operations, such as recommending values and actions over the O1/A1 interface and generating EI for other rApps. rApps enable non-real-time control and optimization of RAN elements and resources, and policy-based guidance for applications in the Near-RT RIC. They can provide functionalities like QoE prediction, traffic pattern prediction, and energy-saving recommendations.

The O-RAN architecture adopts the 3GPP split 2 between the O-CU and O-DU, known as the higher-layer split (HLS) using the F1 interface. Unlike the 3GPP 5G architecture, O-RAN also supports the lower-layer split (LLS), referred to as split 7.2, between the O-DU and O-RU. This utilizes the Open Fronthaul (O-FH) interface for transferring I/Q data samples and scheduling/control messaging between the High-PHY and Low-PHY modules.

The remaining interfaces directly related to RAN control and optimization are E2, A1, and O1. Their characteristics are as follows [2]:

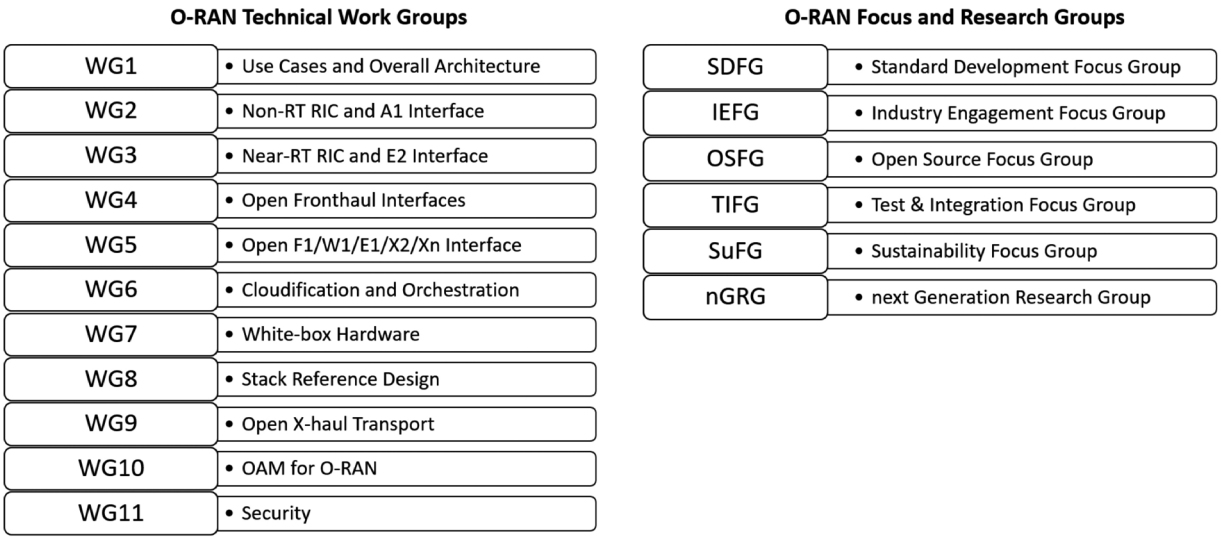
- E2: This interface, between the Near-RT RIC and all E2 Nodes, establishes a closed control loop within the RAN domain. It is used to transmit RIC control and policy decisions from xApps to E2 Nodes and to collect Key Performance Measurements (KPM) from E2 Nodes to provide data for xApps.
- A1: This interface, between the Non-RT and Near-RT RICs, is used to deliver policies, enrichment information (EI), and machine learning (ML) models to the Near-RT RIC, which are then utilized by corresponding xApps. It also facilitates the feedback of policy information back to the Non-RT RIC.
- O1: This interface, between the SMO and O-RAN entities, is used for operations and management, including Fault, Configuration, Accounting, Performance, and Security (FCAPS), as well as Physical Network Function (PNF) software and file management. It allows rApps to receive data from O-RAN nodes and send reconfiguration commands to them.

The architecture of the Near-RT RIC, including its interaction with xApps and operation via the E2 interface, is detailed in [3]. xApps communicate with the Near-RT RIC framework using open APIs. The E2 interface is responsible for transmitting control, indication, and policy messages based on defined service models. These messages' parameters are specified to allow E2 Node providers to expose RAN functionality, enabling xApps to control these functions effectively.

Additionally, the O-RAN ALLIANCE has recently introduced the Y1 interface, which connects the Near-RT RIC to Y1 consumers [2]. This interface enables Y1 consumers to subscribe to or request RAN analytics information services provided by the Near-RT RIC. Y1 consumers could include Application Functions (AFs) within an O-RAN trusted domain. For consumers outside the trusted domain, RAN analytics information can be securely provided via an exposure function. This interface is particularly useful for providing RAN analytics to the 5G core network (CN), which is important in scenarios like V2X and network slicing due to the significant interactions between CN and RAN.

## O-RAN STANDARDIZATION

Looking at the overall approach to specifying Open RAN, there is the 3GPP, which sets the 5G standard encompass-




» *Fig. 2. O-RAN ALLIANCE technical groups*
» *Rys. 2. Grupy robocze zajmujące się technicznymi aspektami w ramach O-RAN ALLIANCE*

ing architecture, radio interface, RAN operation, UE, and core network functionalities. Concerning Open RAN, only certain aspects extend into processing, while others, such as the core network (CN), fall beyond the scope of O-RAN. Within this context, pertinent components include CU, DU, management, orchestration (MANO), and interfaces like E1, F1, etc. Subsequently, there is the O-RAN ALLIANCE, which builds upon the RAN elements defined by 3GPP by introducing E2 and A1 interfaces, both RICs, lower layer split (LLS), a fronthaul solution, and the Service and Management Orchestration (SMO), among others. In doing so, the O-RAN ALLIANCE establishes the O-RAN open architecture. Furthermore, in collaboration with the Linux Foundation, the O-RAN Alliance has established the O-RAN Software Community (OSC), dedicated to developing an open-source software reference design for the entire O-RAN. Additionally, the Telecom Infra Project (TIP) plays a crucial role within the O-RAN domain. Specifically, in the RRM domain, TIP defines the RAN Intelligence and Automation subgroup (RIA), intending to define requirements for use cases prioritized by the operators.

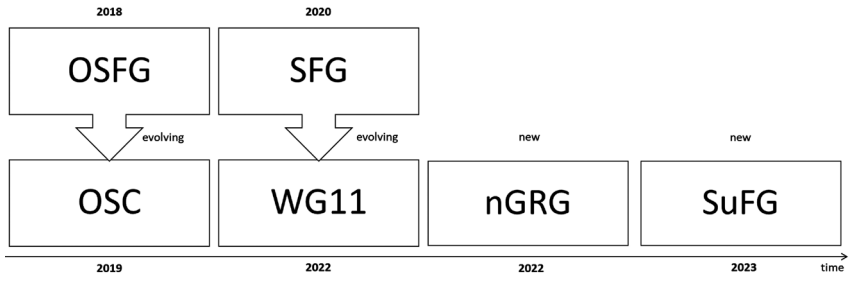
*Fig. 2* provides an overview of the O-RAN ALLIANCE structure related to the technical work. They are split into technical work groups, which cover the standardization of the individual parts of O-RAN architecture, along with focus and research groups, over-arching the technical workgroups or relevant to the whole O-RAN.

The individual O-RAN technical work groups are dealing with the following items:

- WG1 – deals with architecture, network slicing, and use cases;
- WG2 – supports Non-RT RIC internal architecture, and he accompanied protocols and procedures;
- WG3 – defines Near-RT RIC architecture and the relevant E2 interface to control the RAN;
- WG4 – delivers open fronthaul interfaces to realize multi-vendor interoperability between O-DU and O-RU;
- WG5 – provides multi-vendor specifications for 3GPP-based interfaces;
- WG6 – drives the decoupling of hardware and software and provides a reference design for those;
- WG7 – works on the open reference design for the hardware platform;
- WG8 – develops software architecture for O-CU and O-DU;
- WG9 – focuses on transport domain for fronthaul, midhaul, and backhaul network design;
- WG10 – is responsible for Operation Administration and Maintenance (OAM) requirements, architecture, and O1 interface;
- WG11 – focuses on security aspects of the Open RAN architecture.
- On the other hand, the focus and research groups deal with:
- SDFG – focuses on standard development and serves as an interface to standard development organizations like 3GPP or ETSI;
- IEFG – focuses on industry engagement and serves as an interface to the O-RAN ecosystem;
- OSFG – focuses on open source (planning, prep, and establishment of O-RAN Software Community);
- TIFG – focuses on testing and integration, T&I (creates end-to-end T&I specifications, coordinates plugfests, and sets guidelines to O-RAN Test and Integration Centers, OTICs);
- SuFG – focuses on sustainability (energy consumption, efficiency);
- nGRG – conducts research on Open RAN within the 6G framework.

The collaboration between working groups within the O-RAN ALLIANCE involves, e.g., WG1 defining use cases, which establish a framework, signaling flows, measurements, and KPIs. Additionally, they outline the responsibilities of individual O-RAN nodes to fulfill requirements for external applications (xApps and rApps) aimed at optimizing the network for these scenarios. Referring to the use case descriptions provided in the relevant document [4], corresponding specifications such as those for A1 and E2 interfaces are being expanded to incorporate procedures or information elements necessary to support them. In the realm of use cases and the functionality of xApps/rApps, the interaction between the Non-RT and Near-RT RIC is pivotal. These interactions are overseen by two distinct O-RAN ALLIANCE working groups, specifically WG2 and WG3, respectively. Similarly, the work within SuFG on the energy-saving features can then be treated by the O-RAN WG1 to define particular use cases, and WG7, WG10, and WG3 to create particular information elements and procedures to enable those.

One of the important aspects of O-RAN ALLIANCE is that it is a young organization (started its operation in February 2018), thus, in addition to the maturing technical content, it is evolving in this aspect. *Fig. 3* shows the updates to the O-RAN technical groups in recent years.




» *Fig. 3. Evolution of the O-RAN ALLIANCE technical groups*
» *Rys. 3. Ewolucja grup roboczych w ramach O-RAN ALLIANCE*

In 2019, the OSFG work was taken by the OSC which solely creates open-source components of the O-RAN architecture, being a collaboration between O-RAN ALLIANCE and the Linux Foundation. Subsequently, in 2022, the Security Focus Group (SFG), was transformed into a regular working group (WG11) to create normative specifications, as security started to become one of the key topics in O-RAN. Later in the same year, nGRG was created, as one of the key items for O-RAN is to incorporate its concepts natively within the 6G framework. Most recently, as energy efficiency has become one of the key focus areas in mobile networks, SuFG was created and started its operation in 2023.

## CURRENT FOCUS AREAS IN O-RAN

The key focus areas in the current O-RAN ecosystem include security, energy efficiency, 6G, or conflict mitigation. New use cases are also added expanding the O-RAN scope to specific verticals and applications.

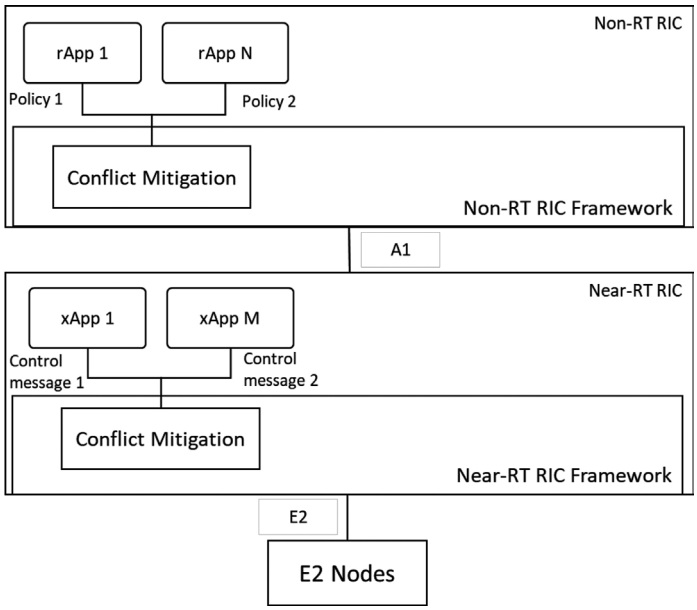
## NEW USE CASES

Comparing the main WG1 use case document versions [4], e.g., from November 2021, and March 2024, one can see, that there were significant updates. Namely, in Nov. 2021, there were 19 use cases identified, and 13 of them analyzed in detail, while in the latest version (Mar 2024), 26 of them were identified, and 19 analyzed in detail. The newest covered energy-saving features, Massive MIMO and MU-MIMO, industrial IoT, security aspects, and network slicing. This later leads to a specification of particular information elements, protocols, and procedures within other O-RAN WGs.

## ENERGY EFFICIENCY

In the RAN, energy efficiency is currently on the agenda of the industry and research activities. O-RAN ALLIANCE is currently providing means to support energy-saving topics as one of the key pillars for moving forward. Quite a several O-RAN WGs focus on energy efficiency topic. WG1 created a technical report [5] covering the key energy-saving use cases which were then incorporated in particular normative specifications within other WGs. The mentioned Network Energy Saving (NES) use cases are:

- Carrier and Cell Switch On/Off – targets the reduction of O-CU/O-DU/O-RU power consumption by switching off/on one or more carriers or a cell. This can be controlled by Non-RT RIC's rApp or Near-RT RIC's xApp;
- RF Channel Reconfiguration Off/On – targets the reduction of power consumption of O-RU with M-MIMO deployment by switching off/on some RF channels. This can be controlled by Non-RT RIC's rApp or Near-RT RIC's xApp;
- Advanced Sleep Mode Selection - targets the reduction of power consumption by partially switching off O-RU components, at a duration of an OFDM symbol, slot, or frame. This can be controlled by Near-RT RIC's xApp;
- O-Cloud Resource Energy Saving Mode - aims to enable energy savings in the O-Cloud by reducing the power consumption of various O-Cloud components without impairing the network performance. This can be controlled by Non-RT RIC's rApp.




» *Fig. 4. Conflict mitigation within RICs*
» *Rys. 4. Łagodzenie konfliktów w ramach modułów RIC*

## CONFLICT MITIGATION

When considering the usage of various functionalities, that control the same RAN nodes, one can notice that there is a potential for conflicts, i.e. when two or more applications would like to guide the RAN in different directions. For example, one application may want to direct a user from one cell to another for the best performance of that user, while at the same time, a different application may want to do the opposite for energy-saving purposes (i.e. wanting to switch off that same cell). For this reason, conflict mitigation is one of the key features, especially within the O-RAN area, where multiple rApps at the Non-RT RIC or xApps at the Near-RT RIC, may come from various vendors and address various use cases at the same time. Currently, it is a hot topic within both WG2 and WG3. Fig. 4 shows an overall O-RAN architecture with those modules present within the RIC frameworks. Besides some commonalities, those mechanisms are somewhat different, i.e. in the Non-RT RIC, the outcome from the rApps is a policy provided towards the A1 interface, thus the conflict mitigation shall address potential conflicts between those policies. As an example here is a Traffic Steering Policy, which could order certain UEs to be associated with a particular cell, while at the same time, the Energy Saving Policy may set the same cell to

move to an energy-saving state. At the Near-RT RIC, on the other end, the xApps directly control the RAN nodes, through control messages, thus the conflict mitigation at that level should resolve conflicts related to particular actions (e.g., two contradicting handover decisions). At this stage of standardization, WG3 already released an initial discussion on conflict mitigation aspects for Near-RT RIC [3], while in WG2 it is still in its emphancy. The latest research papers also touch upon the Near-RT RIC conflict mitigation aspects [6][7][8].

## 6G SYSTEMS

Recently, O-RAN ALLIANCE nGRG released a series of research reports related to how O-RAN fits into the 6G era. An overview of the O-RAN work within the 6G framework is provided in [9] and covers the following requirements and use cases in this context:

- AI/ML deployed in all domains;
- Energy efficiency/saving as a native feature design requirement;
- Disaggregation, openness, modularity, softwarization, and Service-Based Architecture (SBA) as a native approach to future networks;
- Cloud native RAN software;
- Analytics as part of the RAN architecture;
- Real-time network optimization;
- Network support for autonomous mobile robots, drones, extended reality and holographic communication;
- Digital Twins for network efficiency and planning.

The key point is that security, sustainability, and reliability shall be natively embedded in the network design rather than add-ons. It is also envisioned that 3GPP, ETSI, O-RAN ALLIANCE, and other SDOs should work together toward the mobile network evolution [9].

An example study being conducted within nGRG on the enhancements of O-RAN towards its evolution is the so-called "dApps" (distributed Apps) [10]. This concept assumes an execution of real-time control loops operating at timescales below 10 ms. dApps aim at complementing xApps/rApps by allowing operators to implement data-driven management and control directly within the CUs and DUs enabling enabling use cases with strict timing requirements like beam management or scheduling.

## SECURITY

The security topic is a significant part of the O-RAN focus. This is mostly due to the new architecture, more building blocks, and open interfaces which expand the threat space. One such example is the collection of the Near-RT RIC and Non-RT RIC, along with xApps and rApps, which were not present in the traditional RAN. WG11 releasing details on threat analysis and risks [11] requirements [12] and protocol specifications [13]. The research community is also active in this field [14] [15].

Key points currently addressed within this scope include [16] focus on completing security requirements for the decoupled SMO, Near Real-Time RIC and xApps, Open Fronthaul, automated certificate management for CNFs/VNFs, AI/ML security, O-RU centralized user management, and O-Cloud hardening and admission control, as well as further risk assessment and security tests specifications. All of this aims to achieve the goal of Zero Trust Architecture (ZTA).

## CONCLUSIONS

O-RAN ALLIANCE is evolving in terms of the standardization process maturity, integration, and research activities. The ecosystem is also evolving with more players and deployments in place. More and more use cases are being analyzed within O-RAN ALLIANCE for futuristic and advanced use cases like UAV, V2X, IoT, Security, Slicing, and Massive MIMO. O-RAN ALLIANCES's defined use cases are based on prioritization from the operators and are defined as frameworks for xApps/rApps. The key themes for Open RAN include Energy Efficiency, Security, Maturity, Integration, and 6G. One of the challenges and research topics for the RIC is conflict mitigation.

### BIBLIOGRAPHY


[1] O-RAN ALLIANCE, accessed: 2024-05-10. [Online]. Available: https://www.o-ran.or

[2] O-RAN ALLIANCE WG1, *"O-RAN Architecture Description, v.11.0,"* Technical Specification, 03.2024, O-RAN.WG1.OAD-R003-v11.0

[3] O-RAN ALLIANCE WG3, *"O-RAN Near-RT RIC Architecture, v.5.0,"* Technical Specification, 03.2024, O-RAN.WG3.RICARCH-R003-v05.

[4] O-RAN ALLIANCE WG1, *"O-RAN Use Cases Detailed Specification, v.13.0,"* Technical Specification, 03.2023, O-RAN.WG1.Use-Cases-Detailed-Specification-R003-v13.0

[5] O-RAN ALLIANCE WG1, *"O-RAN Network Energy Saving Use Cases Technical Report, v.2.0",* Technical Report, 06.2023, O-RAN.WG1.Network-Energy-Savings-Technical-Report-R003-v02.00

[6] C. Adamczyk and A. Kliks, *"Conflict Mitigation Framework and Conflict Detection in O-RAN Near-RT RIC,"* in IEEE Communications Magazine, vol. 61, no. 12, pp. 199-205, 12.2023, doi: 10.1109/MCOM.018.2200752.

[7] C. Adamczyk and A. Kliks, *"Detection and mitigation of indirect conflicts between xApps in Open Radio Access Networks,"* IEEE INFOCOM 2023 – IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Hoboken, NJ, USA, 2023, pp. 1–2, doi: 10.1109/INFOCOMWKSHPS57453.2023.10225786

[8] Del Prever, P. B., Bonati, L., Polese, M., Tsampazi, M., Lehmann, H., & Melodia, T. (2024). *"PACIFISTA: Conflict Evaluation and Management in Open RAN".* ArXiv. /abs/2405.04395

[9] O-RAN ALLIANCE nGRG, "O-RAN Towards 6G", Research Report, 10.2023 (Report ID: RR-2023-01)
[10] S. D'Oro, M. Polese, L. Bonati, H. Cheng and T. Melodia, *"dApps: Distributed Applications for Real-Time Inference and Control in O-RAN,"* in IEEE Communications Magazine, vol. 60, no. 11, pp. 52–58, 11.2022
[11] O-RAN WG11, *"O-RAN Security Threat Modeling and Risk Assessment v.2.0"*,
[12] O-RAN WG11, "O-RAN Security Requirements and Controls Specification v.8.0",
[13] O-RAN WG11, "O-RAN Security Protocols Specifications v.8.0"
[14] J. Groen et al., "Securing O-RAN Open Interfaces," in IEEE Transactions on Mobile Computing, doi: 10.1109/TMC.2024.3393430
[15] M. Hoffmann and P. Kryszkiewicz, "Signaling Storm Detection in IIoT Network based on the Open RAN Architecture," IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Hoboken, NJ, USA, 2023, pp. 1-2, doi: 10.1109/INFOCOMWKSHPS57453.2023.10226043
[16] O-RAN ALLIANCE, "The O-RAN ALLIANCE Security Working Group Continues to Advance O-RAN Security", 02.2024, [Online]. Available: https://www.o-ran.org/blog/the-o-ran-alliance-security-working-group-continues-to-advance-o-ran-security

DOI: 10.15199/59.2024.4.6

# Efektywne energetycznie wielodostępowe przetwarzanie brzegowe w sieci 5G

## Energy efficient Multi-access Edge Computing in 5G network

dr hab. inż. PAWEŁ KRYSZKIEWICZ
Politechnika Poznańska, Poznań, pawel.kryszkiewicz@put.poznan.pl

STRESZCZENIE Wielodostępowe przetwarzanie brzegowe jest techniką łączącą wykorzystanie sieci komunikacyjnych i oddalonych zasobów obliczeniowych. Pozwala wykonać złożone zadania obliczeniowe na potrzeby urządzeń o niewielkiej mocy obliczeniowej przy zachowaniu niewielkich opóźnień. Istotne jest jednak efektywne zarządzanie przydziałem zadań obliczeniowych do poszczególnych węzłów. W pracy przedstawiono jak system przetwarzania brzegowego może być zintegrowany z siecią 5G, a także jak można rozdzielić zasoby między poszczególne węzły, żeby zminimalizować zużycie energii. Przedstawiony zostanie szereg nowych stopni swobody, które umożliwiają znaczne obniżenie zużycia energii w stosunku do istniejących rozwiązań niezależnej optymalizacji części obliczeniowej i komunikacyjnej.
SŁOWA KLUCZOWE Wielodostępowe przetwarzanie brzegowe, efektywność energetyczna, 5G

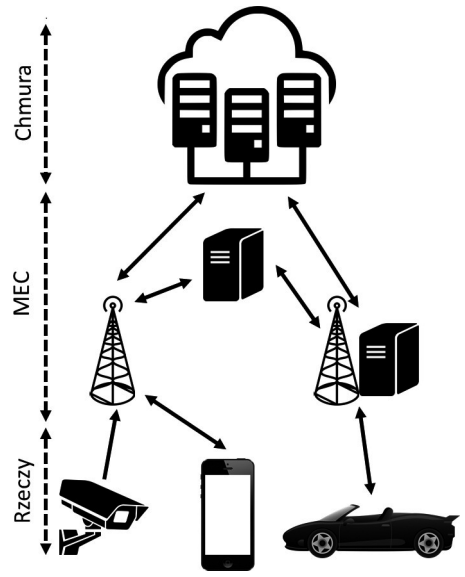
ABSTRACT Multi-access edge computing is a technique that combines the use of communication networks and remote computing resources. It allows to perform complex computational tasks for devices with low computing power while maintaining low latencies. However, it is important to effectively allocate the computing tasks to individual nodes. The work will present how the multi-access edge computing system can be integrated into the 5G network, as well as how resources can be distributed between individual nodes to minimize energy consumption. Some new degrees of freedom will be presented, which enable a significant reduction in energy consumption compared to existing solutions for independent optimization of the computation and communication parts.
KEYWORDS Multi-access Edge Computing, energy efficiency, 5G

Istotą systemów telekomunikacyjnych jest przesył informacji, ale coraz częściej ich źródłem jest urządzenie np. czujnik, a ujściem serwer dokonujący obliczeń albo magazynowania. Ten rodzaj usług jest zwyczajowo nazywany Internetem rzeczy IoT (ang. *Internet of Things*). Taka zmiana jest po części spowodowana zwiększeniem dostępności usług komunikacyjnych, a także obniżeniem kosztu zakupu i utrzymania urządzeń. Istotna jest też zmiana w rodzaju przetwarzania danych. Często dane pochodzące z tanich, zasilanych bateryjnie urządzeń wymagają złożonego przetwarzania z użyciem modeli uczenia maszynowego. Funkcje takie pełni przetwarzanie chmurowe (ang. *cloud*), które jest już powszechnie używane. Trzeba jednak pamiętać, że często chmurowe centra danych oddalone są o tysiące kilometrów od miejsca z którego wysyłane są dane źródłowe. Dodatkowo często po przetwarzaniu jego wynik np. decyzja o wykryciu danego obiektu w strumieniu wideo, musi być użyta lokalnie do podjęcia pewnych akcji. Taka pętla decyzyjna może powodować duże opóźnienia, a także zmienność opóźnienia, co jest nieakceptowalne dla wielu usług, w tym czasu rzeczywistego.

Żeby sprostać tym wymaganiom zaczęto rozważać wykorzystanie niewielkich centrów danych albo pojedynczych komputerów położonych bliżej urządzeń końcowych, które można nazwać „Rzeczami" poprzez odniesienie do „Internetu rzeczy". Taki układ sieci zaprezentowano na *Rys. 1*. Z uwagi na położenie tej warstwy pomiędzy „Rzeczami" oraz chmurą obliczeniową część badaczy odnosi się często do „mgły obliczeniowej" (ang. *Fog computing*) [17]. Jednocześnie podnoszone jest, że dodatkowe węzły obliczeniowe muszą się znaleźć blisko brzegu sieci dostępowej co spowodowało nazwanie tej funkcji wielodostepowym przetwarzaniem brzegowym MEC (ang. *Multiple-access Edge Computing*) [15]. Warto tu podkreślić, że często można znaleźć publikacje, gdzie rozróżnia się przetwarzanie brzegowe od

mgły obliczeniowej z różną granicą podziału. Czasem autorzy sugerują, że mgła to rozrzucone elementy chmury obliczeniowej, a warstwa obliczeń brzegowych odbywa się na samych urządzeniach końcowych. Podnoszone jest też to, że pierwotnie nazwa fog była częściej używana w nawiązaniu do sieci lokalnych LAN (ang. *Local Area Network*), a MEC w odniesieniu do sieci komórkowych. Ciekawym jest też zmiana pierwotnego wyjaśnienia skrótu MEC z „Mobile Edge Computing" na „Multiple-access Edge Computing" przez ETSI w roku 2017 [1]. Miało to podkreślić otwarcie się tworzonych standardów na sieci inne niż komórkowe. Te różnice nomenklaturowe nie są jednak znaczące z perspektywy tego artykułu.

Technologia MEC znajduje wiele zastosowań [5] od przyspieszania przetwarzania strumienia wideo, poprzez obsługę inteligentnych samochodów po technologię rozszerzonej rzeczywistości. Pojawiły się również zmiany w standardach zapewniające jej integrację w ramach architektury sieci 4G albo 5G [2]. Z perspektywy badawczej jednym z problemów jest efektywny rozdział pojawiających się zgłoszeń




» *Rys. 1: Warstwowa architektura brzegowej sieci obliczeniowej MEC*
» *Fig. 1. Multiple Access Edge Computing) i chmury*

obliczeniowych między różne węzły obliczeniowe. Istotna jest tu zarówno część sieciowa (opóźnienie i obciążenie poszczególnych węzłów albo łączy) jak również obliczeniowa (zużycie pojedyncze jednostki obliczeniowe). Efektywność można rozumieć na wiele sposobów. Z pewnością istotne jest zapewnienie użytkownikom usługi w zadanych ramach czasowych (ograniczenie na opóźnienie), ale może być też istotna minimalizacja użycia pewnych węzłów (np. w przypadku taryfikacji o różnym koszcie pracy węzłów obliczeniowych) albo maksymalizacja liczby obsłużonych zadań obliczeniowych [13]. Jednym z istotniejszych podejść jest przydział zasobów minimalizujący, przy zachowaniu wymogów jakościowych, zużycie energii. Poza zmniejszeniem emisji dwutlenku węgla do atmosfery może to znacząco ograniczyć koszty ponoszone przez użytkowników, lub operatorów sieci. Z uwagi na połączenie optymalizacji przesyłu i obliczeń pojawia się wiele dodatkowych zmiennych, które można modyfikować zwiększając potencjalne ograniczenie w zużycia energii.

W tej pracy zostanie przedstawione, jak technika MEC może być zastosowana w sieciach 5G, a także na podstawie wcześniejszych badań autora, jak można przydzielić zadania obliczeniowe w systemie MEC zapewniając minimalizację zużycia energii.

## WIELODOSTĘPOWE PRZETWARZANIE BRZEGOWE W SYSTEMIE 5G

Choć przetwarzanie brzegowe może być zastosowane w różnych sieciach dostępowych, warto tu przedstawić jego połączenie z siecią 5G. Z uwagi na tworzenie architektury 5G oraz architektury MEC prawie równolegle choć przez różne organizacje, są one najbardziej kompatybilne. Oczywiście można by traktować węzły obliczeniowe MEC jako standardowe serwery o pewnych adresach IP. Z perspektywy sieci 5G dostęp odbywałby się jak do innych usług internetowych poprzez scentralizowane User Plane Function (UPF) znajdujące się w sieci rdzeniowej 5G. Nie umożliwiło by to jednak ograniczyć opóźnień na przetwarzanie MEC.

Zarówno ETSI, standaryzując system MEC [7], jak i 3GPP standaryzując sieć 5G [2] zapewniły jednak szereg rozwiązań poprawiających wydajność zastosowania MEc w sieci 5G. Architekturę tego połączenia przedstawiono na *Rys. 2*. Lewa strona rysunku to standardowa architektura sieci 5G przedstawiona z uwagi na oferowane usługi. Po prawej stronie, w ramce, przedstawione są elementy składowe systemu MEC. Płaszczyzna sterująca systemu MEC tzn. MEC Orchestrator, jest połączona z płaszczyzną sterującą sieci 5G będącej szeregiem funkcji np. NEF (ang. *Network Exposure Function*), SMF (ang. *Session Management Function*). Z perspektywy sieci 5G system MEC jest podłączony jako funkcja aplikacji AF (ang. *Application Function*). Pozwala to systemowi MEC na dostęp do wewnętrznych funkcji systemu 5G w tym obserwować parametry radiowe np. jakość sygnału.

Natomiast w płaszczyźnie danych zadanie obliczeniowe pojawiające się w urządzeniu końcowym UE (ang. *User Equipment*) jest przekazywane przez sieć dostępową RAN (ang. *Radio Access Network*) do odpowiedniej instancji funkcji UPF, która jest podłączona do węzłów obliczeniowych (na rysunku ang. *Data network*). Co istotne, może być wiele instancji funkcji UPF w całej sieci. Oznacza to, że dane UE nie muszą być fizycznie przekazane do scenatralizowanego serwera pełniącego rolę sieci rdzeniowej. Instancja UPF może być elementem wybranych stacji bazowych. Może być też zlokalizowana w przełącznikach sieciowych agregujących ruch w sieci 5G. Z uwagi na architekturę opartą na funkcjach można bardzo elastycznie dodawać węzły obliczeniowe blisko urządzeń końcowych wymagających niskiego opóźnienia usług świadczonych przez system MEC. Najbardziej oczekiwana jest instalacja węzłów MEC przez operatorów sieci komórkowych z uwa-

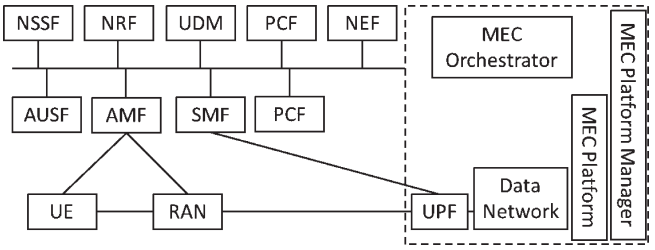
gi na dostępną infrastrukturę w postaci serwerowni, stacji bazowych itp., a także możliwość dywersyfikacji oferowanych usług. Standard MEC umożliwia jednak również integrację zewnętrznych węzłów obliczeniowych. Może mieć to uzasadnienie szczególnie przy braku lokalnej infrastruktury operatora, albo dla ograniczenia kosztów zarządzania węzłami obliczeniowymi. W takim przypadku system MEC nie może być traktowany jako bezpieczny z perspektywy sieci rdzeniowej 5G. Punktem dostępu staje się wtedy funkcja NEF.

Ciekawym aspektem, który postaram się rozwinąć w dalszych rozdziałach artykułu, jest rozdział zadań obliczeniowych między węzły obliczeniowe. Istniejące standardy umożliwiają takie działanie. System MEC przesyła odpowiednie polityki w warstwie sterującej dotyczące konkretnego ruchu tzn. do którego węzła UPF ma zostać przekierowany. Żeby system MEC podjął optymalną albo choć zbliżoną do optymalnej, informację o rozdziale zadań obliczeniowych między węzły musi jednak posiadać pewne informacje o warstwie dostępowej sieci radiowej. Standard przewiduje dostęp do informacji dostępnych nawet w elementach składowych sieci dostępowej tzn. CU (ang. *Centralized Unit*) oraz DU (ang. *Distributed Unit*). Jak zostanie pokazane w następnym rozdziale efektywny przydział zasobów w sieci MEC wymaga informacji np. o opóźnieniach wynikających z użycia konkretnych interfejsów radiowych chociażby poprzez ograniczoną przepływność.

Jako że sieć 5G może obsługiwać szybko poruszających się użytkowników system MEC powinien być również dostosowany do takiej ewentualności np. zapewniając usługi MEC dla komunikacji między pojazdami. W [7] przedyskutowano, jak zapewnić ciągłość usług MEC, zakładając przełączenie między węzłami obliczeniowymi. Najprostsze rozwiązanie może być zapewnione gdy dane zadanie obliczeniowe jest „bezpamięciowe" tzn. węzeł nie musi posiadać informacji o wcześniejszych przesłanych informacjach ani podjętych decyzjach. Można wtedy przenieść zadanie MEC do innej instancji MEC bez koordynacji. W przypadku zadań „pamięciowych" konieczne jest skopiowanie całego stanu danej aplikacji MEC między węzłami obliczeniowymi, a następnie jej uruchomienie. W ten sposób w sieci może pracować kilka identycznych aplikacji. W zadanym momencie jedna z aplikacji jest wyłączana zachowując ciągłość usług. W tym przypadku konieczne jest jednak stworzenie odpowiedniej aplikacji która może być powielona w sieci bez powodowania przekłamań.

## MODELOWANIE SYSTEMU MEC

Przeprowadzenie optymalizacji systemu MEC wymaga zbudowania jego modelu matematycznego z perspektywy interesujących miar jakości oraz zmiennych optymalizacyjnych. Z uwagi na inną naturę przetwarzania inaczej należy również zamodelować część komunikacyjną i przetwarzania brzegowego. Najważniejszymi z perspektywy tego artykułu miarami jakości są opóźnienie czasowe oraz zużycie energii. Trzeba być również świadomym, że modele te muszą stanowić kompromis między dokładnością




» *Rys. 2. MEC zintegrowane z architekturą rdzeniową 5G. Na podstawie: [7]*

odwzorowania rzeczywistych urządzeń i zjawisk, a prostotą optymalizacji.

### Zużycie energii na obliczenia

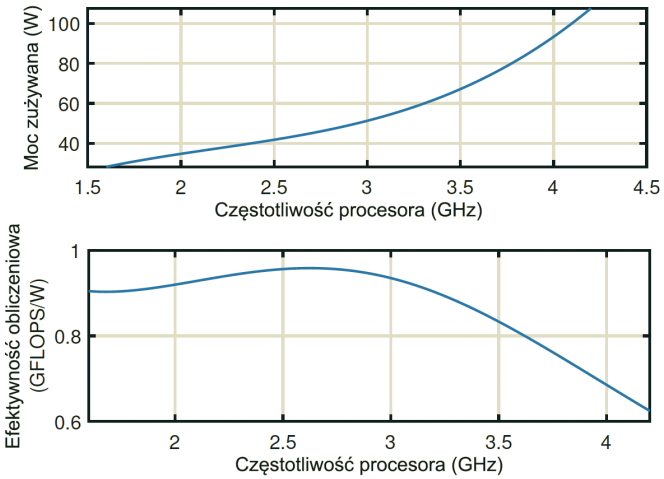
Należy przyjąć, podobnie jak w [9, 8], że pewne zadanie obliczeniowe charakteryzuje się pewną długością $L$ bitów oraz intensywnością zadania $\theta$ wyrażoną w wymaganych operacjach zmiennoprzecinkowych FLOP (ang. *Floating Point Operations*) na bit. Dla danego węzła obliczeniowego można wyznaczyć efektywność obliczeniową $\beta$ wyrażoną w liczbie operacji zmiennoprzecinkowych na sekundę (często oznaczonej jako FLOPS) na Watt. Wypadkowa moc wymagana na przeprowadzenie tych obliczeń wynosi:

$$P_{\mathrm{cp}} = \frac{L\theta}{\beta}. \tag{1}$$

Warto podkreślić, że parametr $\beta$ zależy nie tylko od wykorzystywanej architektury obliczeniowej, ale też konkretnego algorytmu. Zgodnie z rankingiem Green 500, informującej o najbardziej wydajnych superkomputerach, aktualnie osiągane maksimum, na czerwiec 2024 r., to ok. 72 GFLOPS/Watt. Wydajność ta jest zależna m.in. od częstotliwości pracy procesora, a także liczby operacji wykonywanych w jednym cyklu pracy. Co istotne, w pracach [9, 8] pokazano, że można rozważyć dobór optymalnej częstotliwości pracy procesora tzn. $\beta$ jest funkcją (np. wielomianową) częstotliwości taktowania procesora. Przykładowo dla procesora i5-2500K pokazano na *Rys. 3* zmianę efektywności obliczeniowej i mocy zużywanej w funkcji częstotliwości pracy.

Maksymalną efektywność procesor osiąga ok. 2.7 GHz, ale może też pracować z wyższym zegarem osiągając większą szybkość przetwarzania danych, ale przy nieproporcjonalnym wzroście zużycia mocy.

Z perspektywy przydziału zasobów warto zwrócić uwagę, że dla zadań obliczeniowych o łagodnych wymaganiach opóźnieniowych możliwe jest przydzielenie ich do wysokoefektywnych węzłów obliczeniowych. W przypadku zadań wymagających obliczeniowo i czasowo konieczne może być użycie węzła o duże wydajności, a niższej efektywności energetycznej. Dodatkowo można wtedy też podwyższyć częstotliwość taktowania procesora. Może być to też scenariusz konieczny w przypadku dużego obciążenia sieci. Powyższy model może być z powodzeniem używany zarówno dla obliczenia w warstwie MEC jak i w chmurze




» *Rys. 3. Moc używana i efektywność obliczeniowa dla procesora Intel i5-2500K na podstawie [8].*

uwzględniając inne parametry poszczególnych jednostek obliczeniowych.

## Zużycie energii na komunikację

Modelowanie zużycia energii przez sieć komunikacyjną jest dość złożonym problemem. W przypadku sieci bezprzewodowej stosuje się albo modelowanie każdego elementu składowego przetwarzania np. wyprowadza się wzory na zużycie energii przetworników Analogowo-Cyfrowych w danej architekturze i konfiguracji [14] albo przeprowadza się pomiary całych urządzeń uwzględniając możliwe do zmiany parametry np. przepływność użytkowników, odległość użytkowników od punktu dostępowego [10].

Choć pierwsze podejście może mieć więcej punktów swobody, bardziej szczegółowo modelując zużycie energii, rozwiązanie pomiarowe jest częściej stosowane. Wynika to z jego prostoty, a także dużej dokładności przy ograniczonej liczbie parametrów. Wprzypadku modelowania modemów WiFi w [10] zaproponowano parametryzację z uwagi na przepływność (osobno dla nadawania i odbioru) oraz tłumienie propagacyjne między nadajnikiem i odbiornikiem.

Ciekawym aspektem tego modelu jest też uwzględnienie różnic wynikających z architektury czy rozwiązań poszczególnych producentów nawet przy transmisji z użyciem tego samego standardu. W tym celu użyto zmiennych losowych. Podobny model zaproponowało niedawno 3GPP dla stacji bazowych 5G [3]. Zużycie mocy dzieli się na część statyczną i dynamiczną. Część dynamiczna jest skalowana przez procent zajętych zasobów częstotliwościowych, liczbę anten, a także alokowaną moc.

W przypadku przewodowej sieci rdzeniowej, służącej do przesłania zgłoszeń między węzłami MEC oraz chmurą podobny liniowy model zużycia energii jest proponowany [6] tzn. moc stała powiększona o moc zmienną proporcjonalną do obciążenia konkretnego urządzenia sieciowego.

Warto podkreślić, że zarówno w przypadku sieci przewodowej jak i bezprzewodowej zużycie mocy konkretnego urządzenia zależy często od innych zgłoszeń/użytkowników obsługiwanych równolegle, zwiększających obciążenie konkretnych urządzeń. Zakładając, że liczba obsługiwanych urządzeń np. przez konkretny router, jest znacząca należy przyjąć pewne średnie obciążenie i dla tego punktu pracy wyznaczyć wpływ obsługi danego zgłoszenia na zużycie energii. Na podstawie [9] można przyjąć, że całkowita energia potrzebna na transmisję zgłoszenia o długości *L* bitów i przesłania odpowiedzi o długości *oL* bitów wynosi

$$P_{\text{comm}} = L(1 + o)\,(\gamma_{\text{w}} + \gamma_{\text{wl}}) \tag{2}$$

gdzie γw oraz γwl opisuje koszt w Joulach na bit transmisji z użyciem wybranego łącza przewodowego oraz bezprzewodowego.

Warto podkreślić, że dla każdego punktu początkowego i końcowego jest możliwych zazwyczaj wiele dróg o różnym koszcie energetycznym transmisji. Analiza wybranych modeli zużycia energii pozwoliła ustalić w [4] koszt energetyczny transmisji w sieci WiFi ok. 4e4 pJ/b.

Ponad trzy rzędy wielkości wyższe zużycie energii może być oczekiwane od stacji bazowej w sieci LTE. Warto porównać te dwie wartości z energią wymaganą do transmisji jednego bitu wynikająca z Twierdzenia Shannona. Wynosi ona ok. 0.55 pJ. Widać zatem, że istniejące rozwiązania radiowe są jeszcze dość odległe od granicznej efektywności energetycznej. W tym samym artykule pokazano też średnie zużycie energii na bit przez routery przewodowe. W zależności od rodzaju urządzenia to wartość ok. 20–1000 pJ.

## Opóźnienie wynikające z obliczeń

Używając oznaczeń jak w Rozdziale „Zużycie energii na obliczenia" można zdefiniować opóźnienie wynikające z obliczeń jako [8]:

$$D_{\text{cp}} = \frac{L\theta}{fs} \tag{3}$$

gdzie licznik oznacza całkowitą liczbę operacji zmiennoprzecinkowych wymaganych dla danego zadania obliczeniowego, a mianownik definiuje liczbę operacji zmiennoprzecinkowych wykonywanych w ciągu sekundy przez jednostkę obliczeniową, wynikająca z częstotliwości pracy zegara *f* oraz liczby komend wykonywanych w jednym cyklu pracy *s*. Warto podkreślić, że jest to opóźnienie wynikające z samych obliczeń. Ważne też jest dodanie opóźnienia wynikającego z oczekiwania aż poprzednie zadanie obliczeniowe zostanie rozwiązane w danym węźle. Tutaj też ujawni się największa różnica między MEC i obliczeniami chmurowymi. Bardzo duża liczba węzłów w chmurze obliczeniowej pozwala założyć, że zgłoszenia obliczeniowe będą mogły być przypisane do wolnego węzła prawie natychmiast. W przypadku sieci MEC można przypuszczać,

że bliskie, ale ograniczone węzły obliczeniowe będą wymuszały oczekiwanie w kolejce kolejnych zadań.

### Opóźnienie wynikające z komunikacji

Opóźnienie komunikacyjne możemy podzielić na 3 addytywne składowe: opóźnienie wynikające z ograniczonej przepływności łącza, opóźnienie wynikające z odległości między źródłem i ujściem wiadomości oraz opóźnienie wynikające z ograniczeń w dostępie do kanału.

Pierwsze z nich jest wspólne zarówno dla części przewodowej i bezprzewodowej. Dla zadania obliczeniowego o długości $L$ bitów oraz odpowiedzi o długości $oL$ bitów i szybkości bitowej łącza $r$ opóźnienie można wyliczyć jako:

$$D_{\text{comm}} = \frac{L(1+o)}{r}. \tag{4}$$

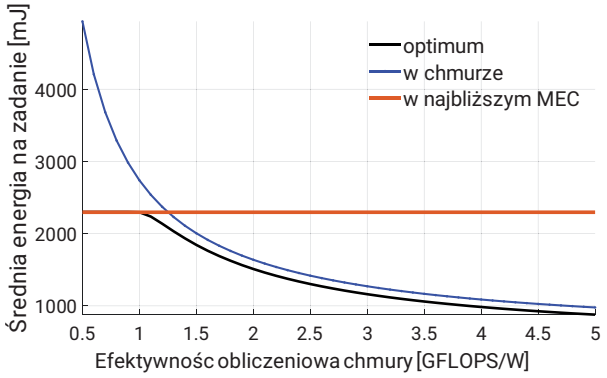
Opóźnienie wynikające z odległości będzie pomijalne przy lokalnych obliczeniach z wykorzystaniem lokalnego węzła MEC. Natomiast w przypadku połączenia z chmurą obliczeniową, odległą o tysiące kilometrów, może być to istotny czynnik. Jak pokazano w [8], to opóźnienie wynosi dla sieci optycznej ok. 7.5 *μs/km*. Poprzez przemnożenie tego współczynnika przez odległość uzyskujemy ten składnik opóźnienia.

Ostatnie z rozważanych źródeł opóźnień jest najbardziej znaczące w przypadku transmisji bezprzewodowej. W wyniku losowego dostępu do kanału (np. WiFi) albo konieczność retransmisji pakietów w następstwie interferencji od innych użytkowników (np. 5G) dane zgłoszenie może dotrzeć do pierwszego węzła sieci MEC opóźnione w sposób losowy. Nie jest to jednak problem z perspektywy problemu przydziału zadań do węzłów obliczeniowych. To opóźnienie już miało miejsce, więc może zostać zmierzone. Musi być jednak uwzględnione. Większym problemem jest opóźnienie w dostępie do łącza przy transmisji odpowiedzi. W artykule [8] założono wykorzystanie sieci WiFi. Używając istniejących modeli matematycznych wyznaczono rozkład opóźnień w dostępie do kanału. Wykorzystano percentyl 98% opóźnienia podczas optymalizacji. Zatem w 98% przypadków powrót odpowiedzi powinien nastąpić przed planowaną chwilą czasu.

## ZINTEGROWANA OPTYMALIZACJA EFEKTYWNOŚCI ENERGETYCZNEJ TRANSMISJI I OBLICZEŃ

Dla tak zdefiniowanej sieci można rozważyć optymalizację alokacji zadania obliczeniowego do odpowiedniego węzła obliczeniowego (w warstwie MEC albo w chmurze), a także zegaru procesora używanego w węźle obliczeniowym. Co istotne, założono, że liczba węzłów MEC jest ściśle ograniczona podczas gdy chmur umożliwia obsługę każdego zadania obliczeniowego na niezależnym węźle. Celem minimalizacja sumarycznej energii wymaganej na obsługę zadań przy założeniu, że każde zgłoszenie ma wyznaczony maksymalny sumaryczny czas obsługi. Jak pokazano w [8], tak zdefiniowany problem należy do klasy MINLP (ang. *Mixed Integer Nonlinear Programming*) z uwagi na występowanie zarówno zmiennych całkowitych tzn. przypisanie zadań do węzłów, a także ciągłych tzn. częstotliwości procesorów. Dodatkowo funkcja opisująca zużycie energii przez procesor może być niewypukła. Problem rozwiązano metodą SCA (ang. *Successive Convex Approximation*) z perspektywy częstotliwości procesora. Użyto również algorytmu węgierskiego dla przypisania zadań do węzłów.

Parametry symulacyjne opisano w [8]. Generowane są

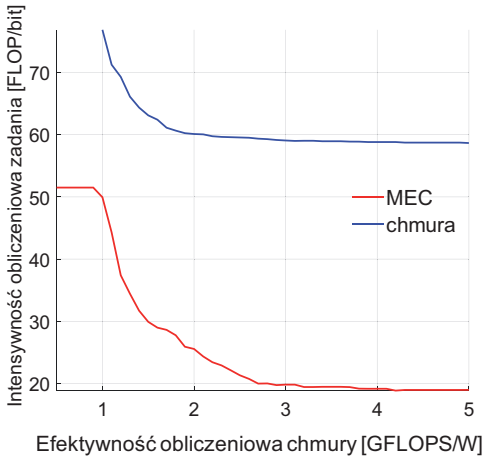



» *Rys. 4. Średnia energia na zadanie obliczeniowe w funkcji efektywności obliczeniowej chmury.*


» *Rys. 5. Procentowy udział MEC w rozwiązywaniu zadań w funkcji efektywności obliczeniowej chmury.*

zgłoszenia óosowej długości, wymaganej intensywności obliczeniowej, a także ograniczeniu na maksymalny czas obsługi. Na *rys. 4* porównano średnią energię zużytą na jedno zadanie obliczeniowe w funkcji efektywności obliczeniowej chmury dla trzech algorytmów przydziału zasobów. W algorytmie przydzielającym zadania tylko w chmurze efektywność obliczeniowa chmury ma znaczący wpływ na koszt energetyczny zadań. Widoczna jest odwrotnie proporcjonalna zależność. Jak można przypuszczać na algorytm przydzielający zadania obliczeniowe najbliższemu węzłowi MEC

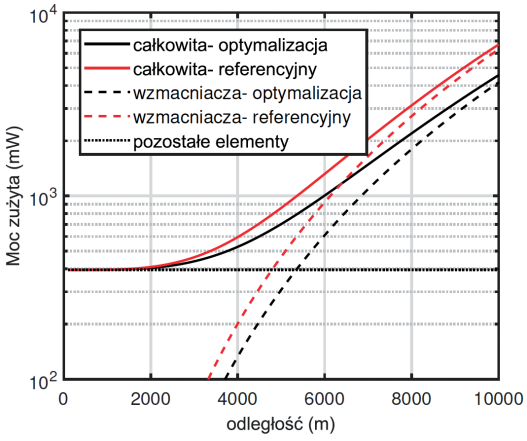
nie ma wpływu zmiana efektywności chmury. Najistotniejsze jest jednak, że zaproponowane rozwiązanie optymalne, dzięki rozdzieleniu zadań między wiele węzłów MEC oraz chmurę może osiągać najniższe średnie zużycie energii na zadanie. Efektywność obliczeniowa chmury ma wpływ na ten przebieg. Co istotne, nawet dla bardzo wydajnej obliczeniowo chmury widoczny jest pewien zysk poprzez wykorzystanie zasobów MEC. Żeby przeanalizować to zjawisko można spojrzeć na *Rys. 5* gdzie pokazane jest procent zadań obliczeniowych wykonywanych w węzłach MEC przy optymalnej alokacji. Choć, zgodnie z oczekiwaniami, 100% zadań obliczeniowych jest wykonywanych w węzłach MEC przy niskiej wydajności obliczeniowej chmury ciekawe jest, że przy bardzo wydajnej chmurze ok. 20% zadań obliczeniowych wykonywane jest w węzłach MEC. Wynika to z części bardzo prostych obliczeniowo zadań, których koszt energetyczny przesłania do chmury może być znaczący. Poparciem tej hipotezy może być *Rys. 6*, który pokazuje średnią intensywność obliczeniową $\theta$ zadań wykonywanych w chmurze i w warstwie MEC. Widoczne jest, że średnio chmura wykorzystywana jest do bardziej złożonych zadań. Nawet przy wyższych efektywnościach obliczeniowych chmury proste zadania (o średniej intensywności obliczeniowej ok. 20 FLOP/bit) są wykonywane w warstwie MEC. Warto tu podkreślić, że powyższa analiza nie rozważa problemu odrzucania zgłoszeń niespełniających wymogów opóźnieniowych. Wpływ tego zjawiska jak również wielu możliwych parametrów przedstawiono w [8].




» *Rys. 6. Średnia efektywność obliczeniowa zadań wykonywanych w chmurze i w węzłach MEC w funkcji efektywności obliczeniowej chmury.*

cji zużycia mocy w sieci MEC uwzględniające dodatkowe, rzadko rozważane zmienne optymalizacyjne. Z perspektywy urządzenia końcowego, często zasilanego bateryjnie, istotne jest obniżenie zużycia energii na przesył zadania obliczeniowego do stacji bazowej lub punktu dostępowego. Choć można w tym celu wykorzystać ogólne metody z perspektywy komunikacyjnej [14], bardziej odpowiednie jest zdefiniowanie tego problemu uwzględniając potencjał obliczeniowy urządzenia końcowego [12]. W przypadku transmisji danych na duże odległości np. z odległych kamer czy czujników IoT, największy udział w zużyciu mocy urządzenia końcowego ma wzmacniacz mocy. Można stosować różne architektury wzmacniaczy, jak również przetwarzanie wstępne sygnału, żeby zwiększyć efektywność energetyczną transmisji [11]. Stosunkowo prostym rozwiązaniem jest dobór punktu pracy wzmacniacza, tak, żeby zmaksymalizować jakość sygnału w punkcie odbioru albo efektywność energetyczną transmisji. Istotnym jest, że taki dobór punktu pracy powoduje pojawienie się zniekształceń nieliniowych w pasmie pracy nadajnika, ale przy zwiększeniu mocy sygnału pożądanego docierającego do odbiornika albo zmniejszeniu zużycia energii na transmisję. Zazwyczaj standardy bezprzewodowe ograniczają poziom zniekształceń po stronie nadajnika np. przez ustalony poziom EVM (ang. *Error Vector Magnitude*), nie jest to jednak optymalne z perspektywy odbiornika.

Stosując metodologię przedstawioną w [12] wyliczono moc zużywaną na wysłanie zgłoszenia obliczeniowe-




» *Rys. 7. Moc zużywana przez urządzenie końcowe na przesył zadań obliczeniowych: scenariusz referencyjny i z optymalizacją punktu pracy wzmacniacza*

## NOWE PERSPEKTYWY OPTYMALIZACJI EFEKTYWNOŚCI ENERGETYCZNEJ SIECI MEC

Jak pokazaliśmy wcześniej, optymalny rozdział zadań między węzły obliczeniowe wraz z uwzględnieniem optymalizacji pracy procesorów pozwala znacząco obniżyć zużycie energii w stosunku do prostszych rozwiązań. Zostaną tu przedyskutowane dwa nowe podejścia do optymalizago (strumienia wideo o przepływności 1 Mbps) do punktu dostępowego. Założono, że transmisja odbywa się na częstotliwości 3.5 GHz z użyciem technologii LTE używającej kanału 20MHz. Poza wzmacniaczem mocy uwzględniono moc zużywaną na kodowanie źródłowe sygnału wideo, kodowanie nadmiarowe, przetwarzanie cyfrowo-analogowe, modulację OFDM, oscylator lokalny, a także mikser. Jak widać na *Rys. 7* moc zużywana przez te komponenty (poza wzmacniaczem mocy) to ok. 400 mW i jest

niezależna od odległości. Widoczne jest, że w większej odległości między nadajnikiem i odbiornikiem moc zużywana przez wzmacniacz jest dominującym składnikiem. Widać też że moc wzmacniacza z optymalizacją punktu pracy jest niższa niż w przypadku systemu referencyjnego, który używa stałego punktu pracy określonej przez IBO (ang. *Input Back-Off*) na 6 dB. Optymalizacja pozwala ograniczyć całkowitą moc zużywaną przez nadajnik o ok. 32% w odległości 10 km.

Ostatnim stopniem swobody, który warto rozważyć przy optymalizacji efektywności energetycznej sieci MEC jest wiek informacji AoI (ang. *Age of Information*) [4]. Często zgłoszenia obliczeniowe wysyłane są do sieci MEC okresowo z danego czujnika. Zwiększenie częstotliwości wysyłania takich danych powoduje zwiększenie wymaganej mocy obliczeniowej, a także zwiększa obciążenie węzłów sieciowych. W sytuacji ekstremalnej może to spowodować skolejkowanie kolejnych zgłoszeń zwiększając dodatkowo wiek informacji w momencie przetwarzania.

Jednocześnie często kolejne dane pomiarowe mogą być silnie skorelowane, a przez to nadmiarowe. Z tej perspektywy sensowne wydaje się minimalizacja częstotliwości przesyłania danych z sensora tak, żeby zapewnić wymagane wskaźniki jakości danej aplikacji (np. wymagane prawdopodobieństwo wykrycia zdarzeń niebezpiecznych przy monitoringu wizyjnym). Wymaga to jednak zbudowania modelu pętli sterowania dla danego typu zastosowania i uwzględnienie jej w globalnym zadaniu optymalizacyjnym sieci MEC. Przykładem może być optymalizacja komunikacji w konwoju pojazdów pod kątem ograniczenia prawdopodobieństwa wystąpienia kolizji między pojazdami [16].

## PODSUMOWANIE

W artykule pokazano, że wykorzystanie systemu MEC może pozwolić zapewnić wiele nowych usług szczególnie wymagających niskich opóźnień. Z perspektywy ograniczenia zużycia energii oraz zapewnienia wysokiej jakości usług MEC konieczny jest wyspecjalizowany przydział zadań obliczeniowych.Wymaga to jednak znajomości modelu całej sieci komunikacyjnej i obliczeniowej, a także możliwości wpływania na konfigurację na wszystkich etapach przesyłu i przetwarzania. Choć jest to zadanie wymagające może znacząco poprawić efektywność działania takiej sieci.

**Praca powstała w ramach projektu OPUS finansowanego przez Narodowe Centrum Nauki nr 2021/41/B/ST7/00136.**

### LITERATURA


[1] Etsi multi-access edge computing starts second phase and renews leadership team". https://www.etsi.o rg/newsroom/news/1180-2017-03-news-etsi-multi-a ccess-edge-computing-starts-second-phase-and-ren ews-leadership-team, dostęp: 2024-06-05.

[2] 3GPP, 2020, „3rd generation partnership project; technical specification group services and system aspects; system architecture for the 5g system (release 15)". Technical Report TS 23.501 V15.10.0, 3GPP.

[3] 3GPP, 2023, „3rd generation partnership project; technical specification group radio access network; study on network energy savings for nr (release 18)". Technical Report TR 38.864 V18.1.0, 3GPP.

[4] Bogucka, Hanna, Kopras, Bartosz, Idzikowski, Filip, Bossy, Bartosz, Kryszkiewicz, Paweł, 2023, „Green time-critical fog communication and computing". *IEEE Communications Magazine*, 61 (12): 40–45.

[5] Hu, Yun Chao, Patel, Milan, Sabella, Dario, Sprecher, Nurit, Young, Valerie, 2015, „Mobile edge computing—a key technology towards 5g". *ETSI white paper*, 11 (11): 1–16.

[6] Idzikowski, Filip, Chiaraviglio, Luca, Cianfrani, Antonio, Vizcaino, Jorge Lopez, Polverini, Marco, Ye, Yabin, 2015, „A survey on energy-aware design and operation of core networks". *IEEE Communications Surveys & Tutorials*, 18 (2): 1453–1499.

[7] Kekki, Sami, Featherstone, Walter, Fang, Yonggang, Kuure, Pekka, Li, Alice, Ranjan, Anurag, Purkayastha, Debashish, Jiangping, Feng, Frydman, Danny, Verin, Gianluca, et al., 2018, „Mec in 5g networks". *ETSI white paper*, 28 (2018): 1–28.

[8] Kopras, Bartosz, Bossy, Bartosz, Idzikowski, Filip, Kryszkiewicz, Paweł, Bogucka, Hanna, 2022, „Task allocation for energy optimization in fog computing networks with latency constraints". *IEEE Transactions on Communications*, 70 (12): 8229–8243.

[9] Kopras, Bartosz, Idzikowski, Filip, Bossy, Bartosz, Kryszkiewicz, Paweł, Bogucka, Hanna, 2023, "Communication and computing task allocation for energy-efficient fog networks". *Sensors*, 23 (2).

[10] Kryszkiewicz, Paweł, Kliks, Adrian, Kułacz, Łukasz, Bossy, Bartosz, 2020, „Stochastic power consumption model of wireless transceivers". *Sensors*, 20 (17): 4704.

[11] Kryszkiewicz, Pawel, Sroka, Pawel, Hoffmann, Marcin, Wachowiak, Marcin, 2023, „Why is white noise not enough? using radio front-end models while designing 6g phy". *Journal of Telecommunications and Information Technology*, (2): 41–45.

[12] Kryszkiewicz, Paweł, Idzikowski, Filip, Bossy, Bartosz, Kopras, Bartosz, Bogucka, Hanna, 2019, „Energy savings by task offloading to a fog considering radio front-end characteristics". *2019 IEEE 30th Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, 1–6.

[13] Luo, Quyuan, Hu, Shihong, Li, Changle, Li, Guanghui, Shi,Weisong, 2021, „Resource scheduling in edge computing: A survey". *IEEE Communications Surveys & Tutorials*, 23 (4): 2131–2165.

[14] Mezghani, Amine, Nossek, Josef A., 2011, „Power efficiency in communication systems from a circuit perspective". *2011 IEEE International Symposium of Circuits and Systems (ISCAS)*, 1896–1899.

[15] Shirazi, Syed Noorulhassan, Gouglidis, Antonios, Farshad, Arsham, Hutchison, David, 2017, „The extended cloud: Review and analysis of mobile edge computing and fog from a security a d resilience perspective". *IEEE Journal on Selected Areas in Communications*, 35 (11): 2586–2595.

[16] Sroka, Paweł, Stro Nm, Erik, Svensson, Tommy, Kliks, Adrian, 2023, „Autonomous controller-aware scheduling of intra-platoon v2v communications". *Sensors*, 23 (1).

[17] Vaquero, Luis M., Rodero-Merino, Luis, 2014, „Finding your way in the fog: Towards a comprehensive definition of fog computing". *SIGCOMM Comput. Commun. Rev.*, 44 (5): 27–32.

# POLITECHNIKA POZNAŃSKA

Cyberbezpieczeństwo sieci radiowych

Łączność satelitarna

Systemy radia kognitywnego

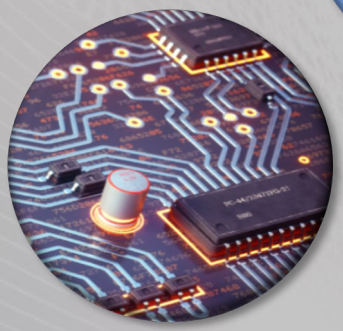
Sieci komórkowe

Zielona telekomunikacja

Komunikacja między pojazdami

Algorytmy warstwy fizycznej

Testowanie układów wielkiej skali integracji



Optymalizacja i ocena wydajności węzłów komutacyjnych w elastycznych sieciach optycznych

Modelowanie i ocena jakości usług w systemach teleinformatycznych

Bezpieczeństwo transmisji w sieciach

Bezpieczeństwo miast inteligentnych

Cyberbezpieczeństwo — techniki MTD

Badania z wykorzystaniem sztucznej inteligencji


**INSTYTUT RADIOKOMUNIKACJI**
ir.put.poznan.pl
office_cr@put.poznan.pl
+61 665 39 30

**INSTYTUT SIECI TELEINFORMATYCZNYCH**
ccn.put.poznan.pl
office_cccn@put.poznan.pl
+61 665 39 20