Cezary Adamczyk
Conflict mitigation in Open Radio Access Networks

Streszczenie

Natychmiastowy, bezprzewodowy dostęp do danych stał się oczywistym przywilejem dla mieszkańców krajów zaawansowanych cyfrowo, stanowiąc fundament sposobu, w jaki nowoczesne społeczeństwo konsumuje media, gromadzi informacje i nawiązuje kontakty społeczne. Aby sprostać temu rosnącemu popytowi i przezwyciężyć ograniczenia konwencjonalnego sprzętu sieciowego – charakteryzującego się zamkniętą konstrukcją, nieprzejrzystymi komponentami typu „black box" i uzależnieniem od jednego dostawcy (zjawisko vendor lock-in) – operatorzy sieci radiowych (ang. Mobile Network Operators, MNOs) coraz częściej wdrażają architekturę otwartej radiowej sieci dostępowej (ang. Open Radio Access Network, O-RAN). O-RAN wprowadza zdezagregowane, zwirtualizowane funkcje sieciowe z otwartymi interfejsami, umożliwiając operatorom wdrażanie stacji bazowych z wykorzystaniem kombinacji sprzętu i oprogramowania od różnych dostawców. Kluczowym elementem tej architektury jest wprowadzenie programowalnej inteligencji do optymalizacji sieci, realizowanej poprzez inteligentne sterowniki sieci (ang. Radio Intelligent Controller, RIC) działające w czasie innym niż rzeczywisty (ang. Non Real-Time RIC, Non-RT RIC) oraz w czasie zbliżonym do rzeczywistego (ang. Near Real-Time RIC, Near-RT RIC). Komponenty te pozwalają na uruchomienie różnorodnych aplikacji, nazwanych rApps i xApps, które umożliwiają operatorom reagowanie na zmieniające się warunki sieciowe i dynamiczną adaptację konfiguracji sieci.

Otwartość i programowalność sieci O-RAN, choć oferuje bezprecedensową elastyczność, wprowadza istotne wyzwania operacyjne w zakresie zarządzania konfliktami. Ponieważ ekosystem O-RAN nie ogranicza się do wybranych dostawców, MNO mogą wdrażać aplikacje xApps i rApps realizowane przez wielu różnych dostawców oprogramowania. Gdy te różnorodne aplikacje działają jednocześnie i modyfikują parametry sieci w celu osiągnięcia potencjalnie odmiennych celów optymalizacyjnych, istnieje wysokie prawdopodobieństwo, że ich decyzje będą wywierać sprzeczny wpływ na konfigurację sieci. Takie konflikty mogą prowadzić do poważnego pogorszenia wydajności sieci i marnotrawstwa zasobów radiowych. Chociaż podobne wyzwania istnieją w innych złożonych architekturach, takich jak systemy operacyjne zarządzające współbieżnymi zadaniami czy sieci Self-Organizing Networks (SON), rozproszona logika w sterownikach RIC tworzy unikalny kontekst, który uniemożliwia bezpośrednie zastosowanie rozwiązań istniejących w innych dziedzinach. Mimo że obecne standardy O-RAN opisują komponent rozwiązywania konfliktów (ang. Conflict Mitigation, ConMit) w Near-RT RIC i wymieniają rozwiązywanie konfliktów jako funkcję wspierającą w Non-RT RIC, nie precyzują one

szczegółowych mechanizmów wykrywania i rozwiązywania konfliktów. W konsekwencji konieczne jest zdefiniowanie uniwersalnego sposobu wykrywania i rozwiązywania konfliktów xApp i rApp, który rozszerzałby architekturę opisaną obecnie w dokumentacji technicznej O-RAN Alliance.

Główną tezą niniejszej rozprawy jest twierdzenie, że mechanizmy rozwiązywania konfliktów mogą znacząco poprawić wydajność, stabilność i niezawodność sieci O-RAN działających z konfliktującymi aplikacjami. Badania opierają się na założeniu, że bez skutecznych środków wykrywania i rozwiązywania konfliktów korzyści płynące z otwartego ekosystemu nie mogą zostać w pełni wykorzystane. W związku z tym głównym celem badań jest zaproponowanie, wdrożenie i ocena kompleksowych ram (frameworku) wykrywania i rozwiązywania konfliktów, które byłyby uniwersalne, solidne i w pełni kompatybilne z architekturą O-RAN. Obejmuje to zaprojektowanie frameworku, który wpisuje się w fundamenty opisane w najnowszych standardach, a jednocześnie pozwala na rozwiązywanie wszystkich typów konfliktów. Badania mają na celu zdefiniowanie ram wykrywania i rozwiązywania konfliktów do wykorzystania zarówno w Near-RT RIC, jak i Non-RT RIC, zapewniając skuteczną neutralizację konfliktów w każdym możliwym scenariuszu sieciowym.

Metodologia przyjęta w niniejszej rozprawie opiera się na systematycznej strukturze, rozpoczynającej się od gruntownego przeglądu literatury, koncentrującego się na standardach O-RAN, raportach technicznych oraz pracach badawczych dotyczących koordynacji funkcji SON, w celu oceny stanu wiedzy. Na podstawie zidentyfikowanych luk badawczych, a w szczególności braku szczegółowej logiki rozwiązywania konfliktów, badania przeszły do etapu konceptualizacji i projektowania ramowego systemu rozwiązywania konfliktów nazwanego Conflict Mitigation Framework (CMF). CMF został zaprojektowany jako proceduralne i agnostyczne pod względem logiki rozwiązanie do wykrywania i rozwiązywania konfliktów w sieciach O-RAN. Aby ocenić korzyści płynące z tego rozwiązania, w ramach badań zaprojektowano i wdrożono autorskie środowisko symulacyjne sieci O-RAN. Oprogramowanie to modeluje środowisko sieci i pozwala na realizację scenariuszy konfliktowych w spójnych warunkach, umożliwiając rzetelny pomiar metryk wydajnościowych (ang. Key Performance Metrics, KPIs).

W ramach proponowanego rozwiązania zaimplementowano wiele algorytmów wykrywania i rozwiązywania konfliktów w celu oceny ich skuteczności. Początkowe etapy koncentrowały się na implementacji konwencjonalnych metod rozwiązywania konfliktów, które posłużyły jako punkty odniesienia (baseline). Następnie badania objęły projektowanie i rozwój rozwiązania opartego na Sztucznej Inteligencji (SI), wykorzystującego konkretnie sztuczne sieci neuronowe (ang. Artificial Neural Networks, ANN) typu aktor-krytyk

(ang. actor-critic) trenowane za pomocą uczenia ze wzmocnieniem (ang. Reinforcement Learning, RL). Podejście to pozwala na adaptacyjne, oparte na danych zarządzanie wykrywanymi konfliktami, zdolne do rozwiązywania złożonych konfliktów sterowania między aplikacjami. Wydajność tych algorytmów została przeanalizowana przy użyciu nowatorskiej metryki ewaluacji, zaproponowanej specjalnie do porównywania rozwiązań dla rozwiązywania konfliktów.

Poza symulacją, rozprawa weryfikuje praktyczność proponowanego rozwiązania poprzez eksperyment przeprowadzony z wykorzystaniem rzeczywistej sieci O-RAN. CMF został zaimplementowany i przetestowany w jednym z laboratoriów certyfikowanych przez O-RAN Alliance dla testów sieci O-RAN, nazywanych O-RAN Open Testing and Integration Center (OTIC). W środowisku testowym wykorzystano rzeczywisty sprzęt i oprogramowanie zgodne ze standardem O-RAN, co zapewnia, że proponowane rozwiązania są skuteczne nie tylko w symulacjach teoretycznych, ale także w rzeczywistej infrastrukturze sieciowej. Ta metodologia testowania, obejmująca projekt teoretyczny, symulację i walidację sprzętową, potwierdza tezę, że solidne rozwiązywanie konfliktów jest kluczowa dla niezawodności sieci O-RAN.

Wyniki badań dostarczają szczegółowego opisu sposobów wykrywania i rozwiązywania konfliktów, wypełniając lukę w obecnych standardach O-RAN. Proponowane rozwiązania stanowią jedne z pierwszych opracowań w obszarze O-RAN poświęconych temu kluczowemu zagadnieniu. Dostarczając wzorca zapewnienia integralności sieci O-RAN w środowisku ze sprzętem i oprogramowaniem od wielu dostawców, praca ta wnosi istotny wkład w rozwój nowoczesnych sieci RAN. Przeprowadzone badania mogą pomóc w określeniu sposobu rozwiązywania problemów z konfliktami sterowania we wszystkich sieciach O-RAN, potencjalnie wpływając na sposób optymalizacji przyszłych sieci RAN i zapewniając, że elastyczność operacyjna O-RAN nie zostanie osiągnięta kosztem stabilności.

Abstract

Instant wireless access to data has evolved into a fundamental, taken-for-granted privilege for populations in digitally advanced nations, fundamentally underpinning how modern society consumes media, gathers information, and socializes. To address this surging demand and overcome the limitations of conventional Radio Access Network (RAN) equipment – characterized by closed designs, opaque "black box" components, and vendor lock-in – Mobile Network Operators (MNOs) are increasingly adopting Open RAN (O-RAN) architectures. O-RAN introduces disaggregated, virtualized network functions with open interfaces, allowing operators to deploy base stations using combinations of hardware and software from various vendors. Central to this architecture is the introduction of robust intelligence for network optimization, implemented through Non-Real-Time (Non-RT) and Near-Real-Time (Near-RT) RAN Intelligent Controllers (RICs). These controllers host diverse applications, known as rApps and xApps, which enable operators to react to changing network conditions and adapt configurations dynamically.

The open and programmable nature of the O-RAN environment, while offering unprecedented flexibility, introduces significant operational challenges regarding conflict management. Because the O-RAN ecosystem is not limited to chosen vendors, MNOs can deploy xApps and rApps implemented by many different software providers. As these various applications operate simultaneously and modify network parameters to achieve potentially distinct optimization goals, there is a high probability that their decisions will exert conflicting influences on how the RICs steer network behavior. Such conflicts can lead to severe network performance deterioration and a waste of vital radio resources. While similar challenges exist in other complex architectures, such as operating systems managing concurrent tasks or Self-Organizing Networks (SON), the distributed nature of O-RAN logic within RICs presents a unique context that prevents the direct application of legacy solutions. Although current standards for O-RAN describe a conflict mitigation component within the Near-RT RIC and list conflict mitigation as a supporting function of the Non-RT RIC, they do not specify the detailed logic for how conflicts should be detected and resolved. Consequently, a universal methodology to detect and resolve control conflicts needs to be defined to extend the architecture currently described by the O-RAN Alliance technical documentation.

The central thesis of this dissertation is that conflict mitigation mechanisms can significantly improve the performance, stability, and reliability of O-RAN networks operating with conflicting applications. The research assumes that without effective detection and resolution measures, the benefits of the open ecosystem cannot be fully exploited. Therefore, the primary purpose of this research is to propose, implement, and evaluate

a comprehensive framework for conflict detection and resolution that is universal, robust, and fully compatible with the O-RAN architecture. This involves designing a framework that fits within the foundation described in the latest standards while allowing for the resolution of all conflict types.

The methodology employed in this dissertation follows a systematic structure, beginning with a thorough literature review of O-RAN standards, technical reports, and research papers on SON function coordination to assess the state of the art. Based on identified research gaps, specifically the lack of detailed logic for conflict resolution, the study progresses to the conceptualization and design of the Conflict Mitigation Framework (CMF). This framework is designed to be a procedural, logic-agnostic solution capable of hosting various conflict detection and resolution algorithms. To assess the benefits of this framework, the research involved the design and implementation of a proprietary O-RAN network simulation environment. This simulation software models the O-RAN environment and allows for the execution of conflict scenarios under consistent conditions, enabling the fair measurement of Key Performance Indicators (KPIs).

Within the proposed framework, the research involved the implementation of multiple conflict detection and resolution algorithms to evaluate their effectiveness. Initial stages focused on implementing conventional conflict resolution methods to serve as baselines. Subsequently, the research advanced to the design and development of an Artificial Intelligence (AI) driven solution, specifically utilizing an actor-critic Artificial Neural Network (ANN) trained via Reinforcement Learning (RL). This approach allows for adaptive, data-driven conflict resolution capable of resolving complex control conflicts between xApps. The performance of these algorithms was analyzed using a novel evaluation metric proposed specifically for the comparison of conflict resolution solutions.

Beyond simulation, the dissertation validates the practical applicability of the proposed solution through hardware-based evaluation. The CMF was implemented and tested in an Open Testing and Integration Center (OTIC), a laboratory for testing O-RAN, certified by the O-RAN Alliance. This testbed utilized real O-RAN-compliant hardware and software, ensuring that the proposed solutions are effective not only in theoretical simulations but also in live network environments.

The results of this research provide a detailed description of how conflict detection and resolution can be achieved, filling the void in current O-RAN standards. The proposed frameworks represent some of the first developments in the O-RAN space dedicated to this critical issue. By providing a blueprint for ensuring network integrity in a multi-vendor environment, this work contributes significantly to the development of modern RAN technology. The conducted research can help determine how conflict mitigation will be

solved in all O-RAN networks, potentially influencing how future RAN networks are optimized and ensuring that the operational flexibility of O-RAN does not come at the cost of stability.