# Analiza możliwości wykorzystywania modelu samosterowania sieci w kontekście systemów otwartych

Julia Skalska and Konrad Olszewski

Contributing authors: 169838@stud.prz.edu.pl; 169826@stud.prz.edu.pl;

**Streszczenie**

W niniejszym artykule przedstawione zostały nowe technologie oraz zagadnienia dotyczące sieci samosterowalnych takie jak Network Function Virutalization (NFV), Cognitive Netowrk, Zero Touch Network czy Open Systems. Uwzględnione zostały również wady a także zalety odpowiednich metod i środków takich jak Artifical Intelligence czy Machine Learning mających zaprowadzić idee samo funkcjonujących sieci do spełnienia. Poruszono również temat bezpieczeństwa tego typu rozwiązań a także przyszłości modelu samosterowalnych sieci jak i systemów otwartych.

**Keywords:** Network Function Virtualization, Zero Touch Network, Artifical Intelligence, Open Systems, Machine Learning

## 1 Wprowadzenie

Świat się rozwija, nowe technologie zostają wprowadzane, toteż nie powinno nas dziwić, że praktyki biznesowe i społeczne ulegają cyfryzacji[1]. To tylko niektóre z nowoczesnych odkryć ostatnich lat.

Transformacja tradycyjnych operacji sieciowych i usługowych w kierunku tych inteligentnych oraz stawania się ich zautomatyzowanymi odbywa się poprzez: wykrywanie anomalii, czyli najpierw następuje monitorowanie w czasie rzeczywistym danych sieciowych, urządzeń, sieci radiowych i szkieletowych oraz usług, transportu i operacji IT. Potem występują korelacje i analiza przyczyn źródłowych, które ukazują pełny obraz sytuacji i umożliwiają zespołom na dotarcie do przyczyny problemu i naprawę, która się obywa za pomocą skryptów automatyzacji. A te jeszcze wymagają obecności człowieka[2]. W tym celu do zwiększenia automatyzacji oraz wirtualizacji sieci

bez ingerencji człowieka powstają nowe metody, pomysły architektoniczne czy technologie. W zagadnieniu sieci, które nie wymagają wkładu ludzkiego do sterowania można wyróżnić takie pojęcia jak Network Function Virtualization (NFV), Cognitive network, Software Defined Network (SDN), Zero Touch Provisioning (ZTP) czy Next-Generation Wireless Networks (NGWN), które zostaną poruszone w poniższej pracy. Duży wkład do pełnego zautoamtyzowania systemów oraz sieci mają w szczególności sztuczna inteligencja oraz uczenie maszynowe, które pozwalają na coraz większe możliwości czy analizę dużej ilości danych a także znajdowanie najbardziej optymalnego rozwiązania problemu.

# 2 Systemy otwarte

Systemy otwarte w przypadku tych komputerowych są połączone z sieciami zewnętrznymi np. z internetem, mogą komunikować się z innymi systemami i korzystać z zewnętrznych usług i zasobów. Oznacza to, że takie systemy, są w stałej interakcji z otoczeniem i wymieniają się informacjami lub energiami między sobą. Pomagają specjalistom z różnych dziedzin współpracować i wprowadzać zmiany w narzędziach, na których polegają. Umożliwiają one również dostosowywanie oprogramowania do indywidualnych potrzeb użytkowników oraz rozwiązanie ogólnych problemów, które nie zostały jeszcze rozwiązane[3]. Systemy otwarte mają wiele zalet i wady. Są to m.in.:

## 2.1 Zalety

Systemy otwarte potrafią dostosowywać się do zmieniających warunków i wymagań, świadczy to o ich elastyczności i skalowalności. Dzięki otwartym interfejsom i wymianie informacji, istnieją większe możliwości integracji z innymi systemami, co sprzyja innowacjom. Dostęp do zewnętrznych zasobów umożliwia efektywniejsze korzystanie z nich, np. z mocy obliczeniowej, pamięci i danych. Natomiast dostęp do usług i rozwiązań zwiększa funkcjonalność systemów i ich możliwości. Czytając artykuł "The Ubiquitous Adoption of Internet Technologies" autorstwa Ina Schieferdecker możemy wyczytać, że systemy otwarte, takie jak oprogramowanie open source, otwarte dane i standardy techniczne mają potencjał poprawy wiarygodności systemów opartych na oprogramowaniu. Umożliwiają one wykorzystanie mądrości tłumu do oceny jakości, bezpieczeństwa i wiarygodności komponentów oprogramowania. Artykuł podkreśla korzyści wynikające z wykorzystania systemów otwartych w budowaniu zaufanych systemów[4].

## 2.2 Wady

Jedną z najważniejszych wad systemów otwartych to ich podatność na ataki i zagrożenia, nie są więc one bezpieczne. Bycie zależnym od innych, zewnętrznych usług jest również ryzykowne pod względem awarii. Zarządzanie takimi systemami może być trudniejsze, wymagać monitorowania i koordynacji z innymi systemami oraz dostawcami usług. Ponadto integracja z różnymi systemami może być skomplikowana, np. gdy występują różnice w specyfikacjach. Ważną wadą jest również brak wsparcia technicznego, które może być ograniczone w porównaniu do komerycyjnych rozwiązań, a

także brak odpowiedzialności, gdyż w przypadku systemów otwartych nie ma jednego dostawcy, który ponosiłby pełną odpowiedzialność za działanie oprogramowania, co może wpływać na wiarygodność i bezpieczeństwo[5].

# 3 Sytemy samosterowania

W dzisiejszych czasach szuka się alternatywnych opcji, by ułatwić pracę człowiekowi w wielu dziedzinach. Coraz więcej rzeczy, czy też właśnie wcześniej wspomnianych operacji sieciowych i usługowych, przechodzą w stronę zautomatyzowanych akcji. W dużej mierze jest to również związane z pojęciem machine learningu, które jest połączone ze sztuczną inteligencją. Uczenie maszynowe to dziedzina informatyki, oferuje ona epidemiologom nowe narzędzia do rozwiązywania problemów. Jej głównym celem jest umożliwienie komputerom "uczenia się" bez bezpośredniego programowania, poprawiając swoją wydajność w zadaniach poprzez doświadczenie, które oznacza w praktyce dopasowanie do danych[6]. Postępy w obszarze sztucznej inteligencji stawarzają natomiast okazję do przyjęcia sieci autonomicznych, które mierzą, analizują i kontrolują się w sposób zautomatyzowany. Wymagane jest również, by przygotowywały sieć na nieoczekiwane zdarzenia[7]. Przed nimi są również wyzwania. Ograniczona wiedza o przyszłych zmianach popytu i środkowiska, w którym działają, a operatorzy sieci oraz użytkownicy nadal nie mają odpowiednich narzędzi do wykorzystania postępów w sztucznej inteligencji[8].

## 3.1 Technologie związane z sieciami samosterującymi

Na ten moment automatyzacja różnego rodzaju systemów czy sieci telekomunikacyjnych jest jednym z większych priorytetów w tej branży. W pomocy z tym przychozdą co raz nowe oraz efektywniejsze rozwiązania. Jednymi z wielu koncepcji dotyczących tego tematu są między innymi:

- Zero Touch Provisioning (ZTP)
- Software Defined Network (SDN)
- Network Function Virtualization (NFV)
- Next-Generation Wireless Networks (NGWN)

W celu zautomatyzowania sieci oraz systemów w samosterowale dużą rolę odgrywa również machine learning jak i sztuczna inteligencja. Powyższe przykłady są jednymi z głównych elementów, które są odpowiedzialne za opiekę nad dużymi sieciami czy systemami[9].

**Next-Generation Wireless Networks (NGWN)**

W tej tematyce przychodzi nam również pojęcie sieci bezprzewodowych nowej generacji (NGWN - Next-Generation Wireless Networks). Dużą rolę ma odgrywać tu szeroka analiza danych, machine learning oraz sztuczna inteligencja, które zwiększają niezawodoność tej sieci a także w ogromnym stopniu przyczyniają się do zmniejszenia kontaktu sieci z administratorem poprzez przejęcie podstawowych operacji oraz wykonywanych usług. Warto również dodać, że takie zastosowania zmniejszają ryzyko wystąpienia pewnych komplikacji czy błędów. Sztuczna inteligencja czy uczenie maszynowe byłyby w stanie zwiększyć także wydajność sieci[10].

**Zero Touch Provisioning (ZTP)**

Kolejnym ważnym pojęciem w automatyzacji sieci oraz systemów jest Zero Touch Provisioning (ZTP). Powiązane jest to z konfiguracją urządzeń sieciowych bez konieczności wykonania tej operacji ręcznie na miejscu. Rozwiązanie to zmniejsza przede wszystkim koszty operacyjne a także pozwala zaoszczędzić czas czy zmniejszyć prawdopodobieństwo wystąpienia błędów podczas ręcznej konfiguracji[11].

**Software Defined Network (SDN)**

Następnym przykładem jest Software Defined Network (SDN). Jest to podejście architektoniczne sieci, która wyodrębnia elementy sterujące urządzeniami sieciowymi w celu przetransportowania ich do głównego miejsca systemu a danemu urządzeniu udostępnienie możliwości tylko używania trywialnych operacji transportowania informacji. SDN znajduje swoje miejsce w sieciach zwirtualizowanych oraz odznaczających się automatyzacją a także w sieciach WAN (Wide Area Network) czy CAN (Campus Area Network)[12].

# 4 Zero touch network

Zero touch network to autonomiczne sieci, które mogą same się naprawiać i dostosowywać w oparciu o sygnały w danych. Zbierają i analizują w ramach całej aktywności sieciowej. Wykorzystują funkcje wirtualizacji, przechodząc na gotowe rozwiązania oparte na oprogramowaniu. Świadczą autonomiczne usługi w zakresie technologii informacyjno-komunikacyjnej. Korzystanie z takich sieci zapewnia bezpieczeństwo systemów zarządzania tą siecią, ale ponieważ istnieje również zagrożenie związane z rosnącą liczbą urządzeń IoT (są to urządzenia obliczeniowe, które łączą się bezprzewodowo z siecią i mają możliwość przysłania danych), usług w chmurze i mobilnych, to sieci muszą być chronione dodatkowymi środkami bezpieczeństwa. Ich celem jest nie tylko jej zabezpieczenie, ale też zachowanie prywatności i integralności danych[13]. Jest to coś innowacyjnego, ponieważ nadal wymagane są ręczne procesy obsługi, a interwencja człowieka jest czymś koniecznym, by zapewnić pełną autonomię do zarządzania siecią i usługami. Ponadto występują ograniczenia, które są motywacją do przyjęcia koncepcji takiej jak Zero Touch Network. Można wyróżnić m.in.:

- złożoność sieci, która zwiększyła się dzięki ogromnej łączności Iot, wielu nowym usługom i nowoczesnym technologiom, takich jak 5G i 6G,
- nowe usługi, a w szczególności te zorientowane na biznes, które trzeba szybko wdrożyć, by sprostać możliwościom w tej dziedzinie,
- poprawa wydajności i potrzeba obniżenia kosztów operacyjnych,
- rewolucja dla sieci "przyszłości", mowa tu nie tylko o sieciach 5G i 6G, ale i także o przyszłej sieci, która będzie bardzo złożona i skomplikowana.

Te ograniczenia wyjaśniają potrzebę koncepcji pełnej automatyzacji i zarządzania przyszłymi sieciami. W celu wyelimionowania tych barier potrzebne są w pełni zaumatyzowane rozwiązania w zakresie obsługi i zarządzania siecią[14].

Automatyzacja zero touch monitoruje: sieci, usługi, reaguje na awarie, a we wczesnym wykrywaniu pojawiających się problemów, autonomicznie się ich uczy, naprawia, podejmuje decyzje i poprawia jakość optymalizacji. Te sieci są oparte na technologii

uczenia maszynowego, która wyszukuje anomalie i również stara się zaradzić wszelkim problemom poprzez analizę przyczyn[15].

Zero touch network and Service Management (ZSM), czyli Bezdotykowe Zarządzanie Siecią i Usługami, to grupa, której celem jest przyspieszenie definiowania wymaganej architektury i rozwiązań typu end-to-end. Została ona utworzona w grudniu 2017 roku w Niemczech, ponieważ założyciele zauważyli potrzebę zmiany sposobu zarządzania i organizowania sieci oraz usług przez sieci 5G i slicing. W szczególności zaistaniała potrzeba wzrostu złożoności, wynikająca z przekształcenia architektury oraz elastyczność operacji wymagana do wspierania nowych możliwości biznesowych. Te potrzebują ogromne pojemności, niezauważalne opóźnienia, wysokie niezawodności, globalny zasięg i poprawę obsługi klienta. Grupa ma na swoim koncie dużo opublikowanych raportów, w których omawiają swoje osiągnięcia[16].

## 4.1 Sztuczna inteligencja jako jeden z pionów automatyczynch sieci

Plany związane z między innymi sieci 5G, 6G czy inne związane są w ogromnym stopniu z pełną automatyzacją. Sieci te miałyby samodzielnie wykonywać dane operacje czy naprawiać usterki bez ingerencji człowieka. Na ten moment sztuczna inteligencja określana jest jako najważniejszy współczynnik w tym temacie. Przewiduje się, że sieci 5G będą rozwiązaniem na wielkie obciążenia sieci przez użytkowników czy opóźnienia transmisji. Z wzrostem wydajności sieci wiąże się również jej złożoność i skomplikowalność co za tym idzie rozwój metod czy technologi mające na celu usprawnienie ich działania. Przykładami ich są między innymi Network Function Virtualization (NFV) czy Software Defined Network (SDN)[17]. Ważnym aspektem jest również Network Slicing. Metoda ta polega na między innymi podziale sieci na segmenty mające na celu obsługiwać określone operacje[18]. Wszystkie te kroki mają na celu zwiększenia wydajności, elastyczności czy zmniejszenia kosztów organizacyjnych związanych z tworzeniem sieci. Na ten moment wielkie znaczenie w tworzeniu w pełni zautomatyzowanych sieci mają machine learning a także sztuczna inteligencja (AL - Artifical Intelligence). Powyższe zagadnienia mają wiele zalet lecz co za tym idzie posiadają także pewne wady. Autorzy artykułu nawiązują do ograniczeń, które systemy działające przy pomocy sztucznej inteligencji muszą spełniać w tym wiedza na temat dlaczego dana procedura zostala wykonana przez AL[19]. Wskazują oni również na ważność posiada szerokiego zbioru danych posiadającego ogromnej klasy informacji, które są przydatne w procesach machine learning do opracowania odpowiednich algorytmów czy sposobów działania[19]. Są one mało spotykane przez to iż w wielu wypadkach są zastrzeżone czy ciężkie do kupienia ze względu na cenę. Kolejnym ważnym aspektem jest umiejętność AL czy machine learningu do wyciągania wniosków oraz zdefiniowania skutków wykonanych operacji co określa to miano interpretowalności. Pomaga to również określić jakie kroki powinny zostać podjęte w przyszłości w przypadku wystąpienia danych rzeczy. Pojęcie podejmowania decyzji można podzielić w tym wypadku na mniej złożone jak i te bardziej co za tym idzie gdzie tworzenie schematu podjętego na bardziej złożonych oraz odchodzących od regularności danych jest bardziej precyzyjne lecz mniej zrozumiałe w przeciwieństwie do prostszego rozwiązania, którego prezycja jest na niskim poziomie[19]. Kolejnym ograniczeniem dotyczącym Machine

Learningu oraz sztucznej inteligencji jest czas ich nauki oraz całkowitego przygotowania do pracy w systemach zautoamtyzowanych czy w tym wypadku na wykonywaniu operacji w 5G, gdzie dane na których działają mogą zmieniać się w szybkim tempie co idzie za ponownym uczeniem się. Warto również dodać, że z wzrostem wydajności systemów oraz sieci zautomatyzowanych opartych na sztucznej inteligencji oraz machine learningu idzie również wzrost wymaganej mocy obliczeniowej do wykonywania operacji. Wiąże się to z nowymi problemami a także potrzebą stałej optymalizacji[19].

# 5 Cognitive network

Technologia sieci danych ogranicza zdolność adaptacji, co wpływa na wydajność. Przekazywanie komunikatu o jej stanie jest tłumione, do elementów nie dociera taka informacja, co skutkuje tym, że jakakolwiek ich reakcja jest ograniczona oraz często odbywa się po wystąpieniu problemu. Tutaj właśnie pojawia się idea sieci kognitywnych, które mają usunąć ograniczenia i pozwolić sieciom działać. Z definicji cognitive network to sieć z procesem poznawczym, która może postrzegać bieżące warunki sieci, planować, decydować i działać na ich podstawie. Uwzględnia ona cele end-to-end, czyli takie, które oznaczają wszystkie elementy sieci, zaangażowane w transmisję przepływu danych[20]. Wszystko, aby podjąć przyszłe decyzje. Bez tych celów i sieci, system może być radiem kognitywnym, które można programować i konfigurować dynamicznie, albo warstwą, działającą na podstawie informacji otrzymanej przez czujniki warstwy fizycznej, ale nie siecią kognitywną. Dla transmisji unicastowej end-to-end może obejmować takie elementy jak podsieci, routery, przełączniki, itd. Ich cele są tym, co odróżnia ją od innych podejść adaptacyjnych, które mają tylko lokalny i jednoelementowy zakres. Sieć kognitywna powinna zapewnić lepszą wydajność end-to-end niż sieć nie kognitywna. Może być wykorzystana do poprawy takich celów jak zarządzanie zasobami, Quality od Service (QoS), bezpieczeństwo, kontrola dostępu, przepustowość. Jest ona ograniczona w zastosowaniu jedynie przez zdolność adaptacji bazowych elementów sieci i elastyczność procesu poznawczego. Jeśli chodzi o koszty takiej sieci, to są one mierzone w kategoriach komunikacji i przetwarzania, wydatków na wdrożenie i utrzymanie architektury oraz złożoności operacyjnej[20].

# 6 Network Function Virtualization (NFV)

Jest to technologia, która daje nowe podejście architektoniczne do tematu związanego z sieciami zautomatyzowanymi, wirtualnymi. Wykorzystuje tradycyjne technologie wirtualizacji sieci.Opiera się również na użyciu maszyn wirtualnych i nie tylko. Pozwala na wyodrębnienie funkcji sieci do oprogramowania pozbywając się w tym przypadku pracy na specjalistycznych urządzeniach. Zastosowanie to umożliwia wiele opcji wprowadzania nowych opcji do sieci. Daje możliwość zaaplikowania ich w jej wielu miejscach. Oddziela oprogramowanie od bazy sprzętowej dając większą elastyczność oraz wiele innych możliwości czy to z aktualizowaniem danych usług czy wprowadzaniem nowych.[21]. NFV wirtualizuje funkcje sprzętu sieciowego[22].

## 6.1 Zalety

Sieci składają się z dużej ilości elementów wliczając to oprogramowanie czy także specjalny sprzęt, którego zakup, optymalizacja czy konfiguracja wiąże się z dużymi kosztami jak i czasem, który należy poświęcić na te operacje. W tym wypadku jedną z ważniejszych zalet NFV jest wirtualizacja funkcji różnego rodzaju sprzętu przez co jego zakup w celu wykonania danej operacji jest zbędny. Kolejną zaletą Network Function Virtualization jest to, że przyczynia się do obniżenia wydatków kapitałowych jak i operacyjnych firmy. Daje również wiekszą elastyczność w wprowadzaniu nowych funkcji do sieci. Przyczynia się również do wzrostu wydajności sieci[22].

Kolejną zaletą NFV jest między innymi zmniejszenie przestrzeni zajmowanej przez sprzęt co jest związane z wirtualizacją odpowiednich funkcji sieciowych co daje również zmniejszenie ilości energi zużywanej przez zastępowaną technologię. Do zalet trzeba również obniżenie wydatków związanych z utrzymaniem kosztów operacyjnych sieci i sprzętu sieciowego. Zastosowanie NFV pozwala również na dłuższą żywotność technologi sieciowej[23].

## 6.2 Wady

Tak jak każdy system czy technologie Network Function Virtualization posiada również wady. Jedną z nich jest zmniejszone bezpieczeństwo. Zwirtualizowane komponenty czy funkcje sieciowe są bardziej podatne na ataki w przeciwieństwie do realnego sprzętu. Wszelkiego rodzaju wirusy czy niebezpieczne oprogramowanie jest trudniejsze do wyodrebnienia i zniwelowania. W tym wypadku technologia wirtualna w porównaniu do realnej jest łatwiejszym celem ataku w przypadku, gdy bezpieczeństwo fizyczne jest tak samo zagwarantowane. Zwirtualizowany sprzęt sieciowy jest prostszym celem niż fizyczne jego modele, które nie muszą być również z sobą połączone. Network Function Virtualization jest narzędziem złożonym przez co potrzebne jest więcej opcji zabezpieczeń w porównaniu do tradycyjnej sieci. Warto również dodać, że ruch sieciowy jest w tym wypadku trudniejszy do analizy czy odczytania[24].

# 7 Przyszłość systemów otwartych i modelu samosterowania sieci

Przyszłość systemów otwartych to zapewne doprowadzenie do automatyzacji i autonomii, będą one zdolne do podejmowania decyzji, dzięki algorytmom uczenia maszynowego, co doprowadzi do minimalizacji potrzeby interwencji człowieka. Oprócz tego takie systemy będą bardziej adaptacyjne i elastyczne, a także będą mogły optymalizaować wykorzystanie zasobów, aby zwiększyć wydajność sieci.

Artykuł "Empowering Self-Driving Networks" przedstawia wizję przyszłości systemów otwartych i samosterujących sieci tak, że wraz z rozwojem technologii sieciowych i programowaloności, sieci stają się coraz bardziej elastyczne, co stwarza możliwość optymalizacji. Natomiast złożoność protokołów sieciowych oraz dynamiczne warunki, w jakich sieci działają, utrudniają jej przeprowadzenie. Samosterujące sieci, które w sposób zautomatyzowany mierzą, analizują i kontrolują siebie, reagując na zmiany w otoczeniu, są już "gotowe" na przyszłe zmiany i zachowują jak największą elastyczność

w czasie, więc artykuł przedstawia argumenty za ich wprowadzeniem. Należy jednak przygotować sieć także na ewentualne nieoczekiwane zdarzenia. Autorzy proponują zastosowanie pojęcia "empowerment" jako miary, która uwzględnia jak "gotowa" jest sieć. Wstępne eksperymenty pokazują, że wykorzystanie empowerment jako czynnika sterującego wyborami działań, pozwala uniknąć wysokich kosztów rekonfiguracji i potencjalnie szkodliwych sytuacji[25].

W przyszłości modelu samosterowania sieci można zauważyć wady i zalety, które będzie ze sobą nieść. Z korzyści można wymienić skalowalność, w zakresie zarządzania i kontrolowania sieci, dostosowywanie się do zmieniających warunków sieciowych, aby zoptymalizować wydajność sieci. Zwiększa się również efektywność operacyjna, model może reagować na problemy w sieci, podejmować odpowiednie działania naprawcze. Ponadto może to pomóc w optymalizacji wykorzystania zasobów sieciowych, zapewnić optymalne korzystanie z dostępnych zasobów. Z wad przede wszystkim należy wymienić potencjalne zagrożenie dla bezpieczeństwa, może być on wykorzystany do cyberataków. Oprócz tego jego złożona implementacja może być skomplikowana, a zarazem problematyczna, co będzie wymagać dobrego zrozumienia i zaplecza technicznego[26].

Systemy otwarte i sieci samosterujące mogą napotkać wiele trudności i ograniczeń, które utrudnią ich skuteczne funkcjonowanie. Wyżej wymienione ataki cybernetyczne, otwarte protokoły i standardy mogą być łatwiejsze do wykorzystania. Rozwinięcie się systemów i sieci może wymagać znacznych nakładów finansowych i zasobów, a wdrożenie i utrzymanie infrastruktury może być kosztowne i czasochłonne. Co więcej niektóre organizacje mogą nie być gotowe na zmianę z tradycyjnych rozwiązań na bardziej innowacyjne. Jeśli chodzi o Network Functions Virtualization (NFV) warto zauważyć, że w niektórych przypadkach może prowadzić do wydajnościowej degradacji sieci. Wirtualizcja wprowadza dodatkowe opóźnienia i zmniejszenie przepustowości, co jest niepożądane w niektórych aplikacjach. Ponadto niektóre przedsiębiorstwa mogą obawiać się utraty kontroli nad swoimi danymi i zasobami w przypadku korzystania z rozwiązań opartych na NFV. Może ona prowadzić do przeniesienia danych i procesów do środowisk wirtualnych, co może być zagrożeniem dla prywatności i bezpieczeństwa.

# 8 Podsumowanie

W artykule omówiony został rozwój i wprowadzenie nowoczesnych technologii, które przyczyniają się do cyfryzacji praktyk biznesowych i społecznych. Skupiliśmy się na temacie sieci zero touch, systemów otwartych i sieci samosterujących. Rozwój nowych technologii, takich jak sztuczna inteligencja, uczenie maszynowe i samosterujące sieci, przyczyniają się do automatyzacji i optymalizacji działań sieciowych. Istnieją także wyzwania, takie jak bezpieczeństwo, zarządanie i brak odpowiednich narzędzi, dlatego dalsze badania i innowacje są potrzebne, aby wykorzystywać dobrze te technologie w sieciach komputerowych. Sieci zero touch wykorzystują techniki monitorowania w czasie rzeczywistym, analizy danych i automatyzacji, aby wykrywać anomalie i rozwiązywać problemy w sieciach, jednak wymagają one wciąż obecności człowieka w procesie naprawy. Systemy otwarte są połączone z zewnętrznymi sieciami i umożliwiają wymianę informacji i zasobów, ale są podatne na ataki i będą

występowały trudności w zarządzaniu, a także braki wsparcia technicznego. Model samosterowania sieci, oparty na sztucznej inteligencji i uczeniu maszynowym, umożliwia zautomatyzowane mierzenie, analizę i kontrolę sieci, jednak istnieją wyzwania związane z ograniczoną wiedzą o przyszłych zmianach. W związku z takimi sieciami omówiliśmy różne technologie, takie jak: Zero Touch Provisioning (ZTP), Software Defined Network (SDN), Network Function Virtualization (NFV) i Next-Generation Wireless Networks (NGWN). Mają one na celu zwiększyć automatyzacje i efektywnoć sieci. Ostatecznie pomimo potencjalnych korzyści, przyszłość systemów otwartych, sieci samosterujących i NFV może nie być odpowiednia dla wszystkich przedsiębiorstw i sytuacji. Złożoność implemenacji, koszty i wymagania dotyczące bezpieczeństwa, musi zostać uwzględniona przed podjęciem decyzji o ich wdrożeniu.

# Literatura


[1] Zero Touch Networks: Opportunities, Challenges and Potential Applications | IEEE Communications Society. https://www.comsoc.org/publications/magazines/ieee-network/cfp/zero-touch-networks-opportunities-challenges-and-potential Accessed 2023-05-07

[2] What is a Zero Touch Network? https://www.anodot.com/learning-center/zero-touch-network/ Accessed 2023-05-07

[3] Montenegro, D., Dugan, R., Taylor, J., McGranaghan, M.: Open-source software projects for advancing the power systems analysis. In: 2022 Open Source Modelling and Simulation of Energy Systems (OSMSES), pp. 1–6. IEEE, Aachen, Germany (2022). https://doi.org/10.1109/OSMSES54027.2022.9768968 . https://ieeexplore.ieee.org/document/9768968/ Accessed 2023-05-07

[4] Schieferdecker, I.: Trustworthiness of Open Source, Open Data, Open Systems and Open Standards. In: 2012 IEEE 36th Annual Computer Software and Applications Conference, pp. 82–82. IEEE, Izmir, Turkey (2012). https://doi.org/10.1109/COMPSAC.2012.104 . https://ieeexplore.ieee.org/document/6340126/ Accessed 2023-05-07

[5] Montenegro, D., Dugan, R., Taylor, J., McGranaghan, M.: Open-source software projects for advancing the power systems analysis. In: 2022 Open Source Modelling and Simulation of Energy Systems (OSMSES), pp. 1–6. IEEE, Aachen, Germany (2022). https://doi.org/10.1109/OSMSES54027.2022.9768968 . https://ieeexplore.ieee.org/document/9768968/ Accessed 2023-05-07

[6] Bi, Q., Goodman, K.E., Kaminsky, J., Lessler, J.: What is Machine Learning? A Primer for the Epidemiologist. American Journal of Epidemiology, 189 (2019) https://doi.org/10.1093/aje/kwz189 . Accessed 2023-05-07

[7] Kalmbach, P., Zerwas, J., Babarczi, P., Blenk, A., Kellerer, W., Schmid, S.: Empowering Self-Driving Networks. In: Proceedings of the Afternoon Workshop on Self-Driving Networks, pp. 8–14. ACM, Budapest Hungary (2018). https://doi.org/10.1145/3229584.3229587 . https://dl.acm.org/doi/10.1145/3229584.3229587 Accessed 2023-05-07

[8] Jacobs, A.S., Pfitscher, R.J., Ferreira, R.A., Granville, L.Z.: Refining Network Intents for Self-Driving Networks. In: Proceedings of the Afternoon Workshop on Self-Driving Networks, pp. 15–21. ACM, Budapest Hungary (2018). https://doi.org/10.1145/3229584.3229590 . https://dl.acm.org/doi/10.1145/3229584.3229590 Accessed 2023-05-07

[9] Babaei, A., Kebria, P.M., Nahavandi, S.: A survey on Automation Technologies used in Network Control and Management. In: 2022 15th International

Conference on Human System Interaction (HSI), pp. 1–6. IEEE, Melbourne, Australia (2022). https://doi.org/10.1109/HSI55341.2022.9869444 . https://ieeexplore.ieee.org/document/9869444/ Accessed 2023-05-07

[10] Babaei, A., Kebria, P.M., Nahavandi, S.: A survey on Automation Technologies used in Network Control and Management. In: 2022 15th International Conference on Human System Interaction (HSI), pp. 1–6. IEEE, Melbourne, Australia (2022). https://doi.org/10.1109/HSI55341.2022.9869444 . https://ieeexplore.ieee.org/document/9869444/ Accessed 2023-05-07

[11] Zero Touch Provisioning - What is it and is it useful for me? (2019). https://www.nomios.pl/en/news-blog/what-is-zero-touch-provisioning/ Accessed 2023-05-07

[12] Guzenda, M.: Sieci SDN - Co To Jest Software-Defined Networking? (2020). https://marcelguzenda.pl/co-to-jest-sdn/ Accessed 2023-05-07

[13] Zero Touch Networks: Opportunities, Challenges and Potential Applications | IEEE Communications Society. https://www.comsoc.org/publications/magazines/ieee-network/cfp/zero-touch-networks-opportunities-challenges-and-potential Accessed 2023-05-07

[14] Liyanage, M., Pham, Q.-V., Dev, K., Bhattacharya, S., Maddikunta, P.K.R., Gadekallu, T.R., Yenduri, G.: A survey on Zero touch network and Service Management (ZSM) for 5G and beyond networks. Journal of Network and Computer Applications **203**, 103362 (2022) https://doi.org/10.1016/j.jnca.2022.103362 . Accessed 2023-05-07

[15] What is a Zero Touch Network? https://www.anodot.com/learning-center/zero-touch-network/ Accessed 2023-05-07

[16] Dahmen-Lhuissier, S.: Zero touch network & Service Management (ZSM). https://www.etsi.org/technologies/zero-touch-network-service-management?jjj=1681479270952 Accessed 2023-05-07

[17] Benzaid, C., Taleb, T.: AI-Driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions. IEEE Network **34**(2), 186–194 (2020) https://doi.org/10.1109/MNET.001.1900252 . Accessed 2023-05-07

[18] Corporation, C.: What Is Network Slicing? - Blue Planet. https://www.blueplanet.com/resources/what-is-network-slicing.html Accessed 2023-05-07

[19] Benzaid, C., Taleb, T.: AI-Driven Zero Touch Network and Service Management in 5G and Beyond: Challenges and Research Directions. IEEE Network **34**(2), 186–194 (2020) https://doi.org/10.1109/MNET.001.1900252 . Accessed 2023-05-07

[20] Arslan, H.: Cognitive Radio, Software Defined Radio, and Adaptive Wireless Systems. Signals and Communication Technology Ser. Springer, New York (2007)

[21] Yong Li, Min Chen: Software-Defined Network Function Virtualization: A Survey. IEEE Access **3**, 2542–2553 (2015) https://doi.org/10.1109/ACCESS.2015.2499271 . Accessed 2023-05-07

[22] Kaur, K., Mangat, V., Kumar, K.: Architectural Framework, Research Issues and Challenges of Network Function Virtualization. In: 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 474–478. IEEE, Noida, India (2020). https://doi.org/10.1109/ICRITO48877.2020.9197802 . https://ieeexplore.ieee.org/document/9197802/ Accessed 2023-05-07

[23] Corporation, C.: What is Network Function Virtualization (NFV) - Blue Planet. https://www.blueplanet.com/resources/What-is-NFV-prx.html Accessed 2023-05-07

[24] What is Network Functions Virtualization (NFV)? | VMware Glossary. http://www.vmware.com/topics/glossary/content/network-functions-virtualization-nfv.html Accessed 2023-05-07

[25] Kalmbach, P., Zerwas, J., Babarczi, P., Blenk, A., Kellerer, W., Schmid, S.: Empowering Self-Driving Networks. In: Proceedings of the Afternoon Workshop on Self-Driving Networks, pp. 8–14. ACM, Budapest Hungary (2018). https://doi.org/10.1145/3229584.3229587 . https://dl.acm.org/doi/10.1145/3229584.3229587 Accessed 2023-05-07

[26] Montenegro, D., Dugan, R., Taylor, J., McGranaghan, M.: Open-source software projects for advancing the power systems analysis. In: 2022 Open Source Modelling and Simulation of Energy Systems (OSMSES), pp. 1–6. IEEE, Aachen, Germany (2022). https://doi.org/10.1109/OSMSES54027.2022.9768968 . https://ieeexplore.ieee.org/document/9768968/ Accessed 2023-05-07