Projekt realizowany w konkursie CYBERSECIDENT

CYBERSECIDENT/487845/IV/NCBR/2021

Zaawansowane metody i techniki
wykrywania i przeciwdziałania atakom
na infrastrukturę dostępową i aplikacje sieci 5G

P6.1 Projekt Techniczny Systemu 5gSTAR

WIŁ-PIB, Politechnika Poznańska, Grandmetric

Wersja: **1.0**

Wykonał: **Dr inż. Przemysław Bereziński**

Zadanie: **A6**

Data: **30.07.2024**

REJESTR ZMIAN

Lp.	Wersja	Data	Wprowadzający	Opis zmiany
1	1.0	30.07.2024	P.Bereziński	

SPIS TREŚCI

1 WSTĘP

Niniejszy raport zawiera wkład do Projektu Technicznego Systemu 5gSTAR stanowiący Produkt P6.1 etapu A projektu 5gSTAR [1]. Struktura dokumentu jest następująca:

Rozdział 1 – Wstęp,

Rozdział 2 – Stos technologiczny,

Rozdział 3 – Platforma 5G,

Rozdział 4 – Projekt ogólny,

Rozdział 5 – Specyfikacja,

Niniejszy raport nie zawiera aktualnych wymagań na System 5gSTAR. Są one zdefiniowane w osobnym dokumencie pt. „Weryfikacja wymagań na system 5gSTAR" [6].

2 STOS TECHNOLOGICZNY

2.1 DETEKTORY OPRACOWANE W RAMACH PROJEKTU

Autorskie detektory ataków opracowane w Systemie 5gSTAR będą uruchamiane na systemach operacyjnych Linux bazujących na dystrybucji Ubuntu oraz Fedora (stacja bazowa i siec rdzeniowa 5G Amarisoft, oraz Open5GS). Należy podkreślić, że istnieje możliwość uruchomienia ich także na innych systemach operacyjnych w tym Windows. Jako język programowania do implementacji detektorów opracowanych w ramach projektu tj. detektorów zagłuszania, detektorów ataków typu odmowa usługi oraz detektorów anomalii w sieci przemysłowej SCADA (ang. *Supervisory Control and Data Acquisition*) i IIoT (ang. *Industrial Internet of Things*) wybrano język Python 3. Wybór podyktowanym był m.in.:

- dużą popularnością i powszechna znajomością tego języka wśród programistów, co miało potwierdzenie w zespole realizującym 5gSTAR,

- bogatym zestawem bibliotek i frameworków (zarówno standardowych jak i specjalistycznych np. dla uczenia maszynowego) oraz dużą społecznością, co pozwala na znaczną oszczędność czasu przy tworzeniu oprogramowania,

- intuicyjną składnią i przejrzystością kodu, co daje możliwość tworzenia oprogramowania dla programistów o różnym poziomie umiejętności,

- możliwością stosowania różnych paradygmatów programowania (proceduralne, obiektowe, funkcyjne), co zapewnia dużą swobodę i elastyczność, a co najważniejsze dla Projektu pozwala wykorzystać programistów z różnym tłem i doświadczeniem,

- wieloplatformowością (ten sam kod działa na różnych systemach operacyjnych – zgodnie z zasadą „*write once, run anywhere"*),

- możliwością szybkiej integracji z gotowymi rozwiązaniami informatycznymi i innymi językami programowania.

Kwestie nieco gorszej szybkości działania programów napisanych w Python niż np. w C/C++, czy nawet Java i C# (kod Python jest interpretowany, a nie kompilowany) zostały zaakceptowane przez zespół realizujący Projekt. Należy zaznaczyć, że elementy detekcji w Systemie 5gSTAR nie działają w trybie *„inline"* tylko na kopii danych co powoduje, że nie wpływają na jakość usług w sieci 5G (nie wprowadzają opóźnień i błędów).

2.2 Detektory Uzupełniające

W systemie 5gSTAR zaplanowano także wykorzystanie gotowych detektorów tzw. podejście COTS (ang. *Commercial Off the Shelf*). Detektory te przy odpowiednim dostrojeniu i rozszerzeniu o autorskie reguły detekcji mają uzupełniać autorskie metody. Takie hybrydowe podejście pozwala na poniesienie poziomu detekcji i obniżenie poziomu fałszywych alarmów przy detekcji ataków. Gotowe detektory, które zastosowano to system wykrywania intruzów SNORT (www.snort.org) oraz system pułapkowy Conpot (conpot.org). Wybór tych rozwiązań wynikał z ich popularności oraz możliwości rozbudowy i dostrojenia do potrzeb systemu 5gSTAR.

2.3 System Monitorowania

Jako platformę do budowy systemu monitorowania wybrano Elastic Stack. Jest to otwarta platforma (ang. *open source*) służąca do akwizycji, agregacji, analizy i wizualizacji danych. Elastic Stack jest często wybierany w projektach informatycznych jako darmowa alternatywa dla rozbudowanych narzędzi do monitorowania sieci tzw. SIEM (ang. *Security Information and Event Management*) takich jak np. Splunk (www.splunk.com) czy Q-Radar (https://www.ibm.com/qradar). Zespół realizujący projekt 5gSTAR zadecydował, że wybór Elastic Stack będzie odpowiedni ze względu na wystarczająca funkcjonalność, dużą elastyczność, odpowiednią wydajność i bezpieczeństwo oraz doświadczenie wynikające z

udanych wdrożeń tego rozwiązania przez zespół realizujący Projekt (głównie Grandmetric). Nie bez znaczenia był też fakt, że Elastic Stack jest stosowany w poważnych realizacjach o podobnym charakterze m.in. przez Deutsche Telekom [7] czy Verizon Wireless [8]. Elastic Stack to zintegrowany zestaw narzędzi pozwalający na przetwarzanie i analizę dużych ilości danych (ang. *big data*). Składa się z takich komponentów jak: Elasticsearch, Logstash, Kibana i Beats.

Elasticsearch jest serwerem wyszukiwania i analityki i jest centralną częścią Elastic Stack. Pozwala na przechowywanie i wyszukiwanie danych w krótkim czasie. Oferuje wiele funkcjonalności m.in.: filtrowanie, sortowanie, agregacja i wyszukiwanie pełnotekstowe, a także automatycznie skalowanie w zakresie przechowywania i przetwarzania większych ilości danych. Efektywność przetwarzania zapytań w Elastic Stack zależy od wielu czynników, takich jak rozmiar klastra, możliwości sprzętowe serwerów, ilość danych w klastrze, typ i złożoność zapytań. W zaproponowanym dla systemu 5gSTAR rozwiązaniu wykorzystującym rozwiązanie sprzętowe zakupione w Projekcie zapewniona będzie odpowiednia wydajność przy jednoczesnej ochronie danych w sytuacjach awaryjnych (klaster typu gorąca rezerwa).

Kibana to interfejs użytkownika, który pozwala na wizualizację i analizę danych przechowywanych w Elasticsearch. Kibana oferuje wiele narzędzi, takich jak interaktywne wykresy, diagramy, mapy i tabele, które pozwalają na łatwe zrozumienie i analizę danych (podejście kognitywne). Kibana wraz z modułami rozszerzającymi będzie stanowić główny interfejs dla operatora Systemu 5gSTAR.

Akwizycja i wstępne przetwarzanie danych w Systemie 5gSTAR będzie realizowane poprzez Logstash i Beats. Logstash pozwala na przetwarzanie logów (parsowanie, filtrowanie), i przesyłanie ich w postaci ustrukturyzowanych zdarzeń do Elasticsearch. Beats to rodzaj lekkiego agenta instalowanego na hostach do zbieranie logów, metryki i danych sieciowych w celu przekazania ich do Logstash lub Elasticsearch.

2.4 MITYGACJA

Łagodzenie skutków ataków będzie realizowane wieloetapowowo. Zarządzanie procesem mitygacji ma być realizowane przez dedykowane oprogramowanie APA (Aplikacja Przeciwdziałania Atakom) opracowywane przez WIŁ-PIB (framework Django dla Python) i Grandmetric (framework Flask + biblioteka PyVibe dla Python). Detektory dla ataków w warstwie radiowej tj. *jamming*, *signalling storm* maja posiadać wbudowane funkcje

automatycznego łagodzenia ataków napisane w języku Python. Dla innych zagrożeń zakłada się opracowanie skryptów mitygujących atak (Linux Bash/ Python) i instrukcji postępowania na bazie TTP (ang. *Tactics, Techniques, Procedures*) modeli MITRE FiGHT i ATT&CK [2].

3 PLATFORMA 5G

Wybór platformy 5G poprzedzono przeglądem rozwiązań dostępnych na rynku. Analizowano zarówno rozwiązania darmowe jak i komercyjne o charakterze badawczym. Informacje na temat docelowo wybranej platformie znajdują się w Rozdziale 4.

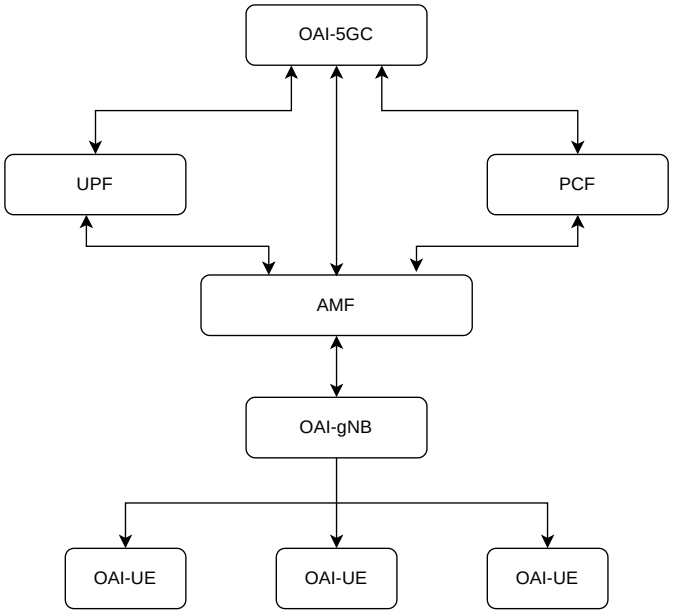
3.1 OPENAIRINTERFACE

Od kilku lat można zaobserwować wyraźny wzrost zainteresowania rozwojem oprogramowania na licencji open-source umożliwiającego prowadzenie badań nad częścią dostępową i szkieletową sieci komórkowych. Do takich bibliotek oprogramowania open-source należą narzędzia m.in. OpenAirInterface (OAI) [9] i srsRAN [10]. Wspomniane pakiety oprogramowania są używane w połączeniu z urządzeniami radiowymi definiowanymi programowo (ang. *Software Defined Radio* - SDR). Umożliwiają szybkie uruchomienie w pełni funkcjonalnych elementów sieci komórkowej, które są zgodne ze standardem i kompatybilne z komercyjnymi telefonami komórkowymi, a funkcjonują na zasadzie licencji otwartych. Wspomniane rozwiązania wpisują się w pomysł tworzenia sieci dostępowej zgodnie z koncepcją Open Radio Access Network (O-RAN) [11]. Wraz z pojawieniem się sieci 5G zaczęła bowiem funkcjonować koncepcja tworzenia sieci dostępowej w łączności telefonii komórkowej niezależnej od oprogramowania jednego dostawcy, tak jak miało to miejsce w poprzednich generacjach telefonii komórkowej. Wprowadzenie środowiska O-RAN dla sieci 5G jest inicjatywą prowadzoną przez projekt Telecom Infra, która koncentruje się na definiowaniu rozwiązań dostępowej sieci radiowej (ang. *Radio Access Network* - RAN) opartych na uniwersalnym oprogramowaniu, niezależnym od konkretnych dostawców, które nie jest ograniczone prawami własności. Według idei O-RAN interfejsy urządzeń wchodzących w skład sieci radiowej są otwarte. Pozwala to na korzystanie ze sprzętu różnych dostawców, oprogramowanie jest niezależne od dostawców. Inicjatywa ma na celu przyspieszenie wprowadzania innowacji w sieci RAN. Oprogramowanie O-RAN działa głównie na serwerach typu whitebox, wykorzystywane jest m.in. w narzędziach srsRAN i OpenAirInterface. Narzędzia te pozwalają projektować i budować prototypy, analizować i testować nowe rozwiązania w rzeczywistych środowiskach.

Narzędzie OpenAirInterface jest szeroko używane w środowisku akademickim i przemysłowym do testowania i prototypowania nowoczesnych technologii sieciowych. Realizuje protokoły należące do stosu protokołów definiowanych przez organizację 3GPP. Emuluje działanie elementów radiowej sieci dostępowej telefonii komórkowej 4 i 5 generacji: eNB, gNB i 4G, 5G UE, oraz sieci szkieletowej: EPC (ang. *Evolved Packet Core*) i 5G-CN (ang. *5G Core Network*). Kod źródłowy projektu OpenAirInterfaceTM (OAI) jest podzielony na trzy główne komponenty: sieć dostępu radiowego OAI (OAI- gNodeB), sieć szkieletową OAI (OAI-5GC), wyposażenie użytkownika OAI (OAI-UE).

Moduł dostępowej sieci radiowej jest dostępny na portalu GitLab: https://gitlab.eurecom.fr/oai/ openairinterface5g/. Realizuje przede wszystkim funkcje stacji bazowej gNodeB, zarządzanie zasobami radiowymi, harmonogramowanie oraz połączenia z urządzeniami użytkownika (ang. *User Equipment* - UE).

Moduł sieci szkieletowej OAI (OAI-CN) jest dostępny na portalu GitHub: https://github.com/ openairinterface. Realizuje sieć szkieletową 4 i 5 generacji. M.in. realizuje wybrane funkcje architektury sieci szkieletowej 5G. Funkcję AMF (Access and Mobility Management Function), która zarządza dostępem i mobilnością użytkowników, funkcję SMF (Session Management Function) zarządzającą sesjami danych, funkcję UPF (User Plane Function) przetwarzającą dane użytkowników, funkcję PCF (Policy Control Function) zarządzającą politykami sieci, np. sposobem rozliczania użytkowników za realizowane usługi, funkcję AUSF (Authentication Server Function) odpowiedzialną za uwierzytelnianie użytkowników. Moduł wyposażenia użytkownika - User Equipment (OAI-UE) realizuje funkcje urządzenia użytkownika 5G, symuluje działanie terminala 5G, obsługując wszystkie niezbędne warstwy protokołów urządzenia końcowego. Projekt jest dostępny pod adresem: https://openairinterface .org/. Schemat architektury systemu OpenAirInterface emulującego działanie sieci 5G przedstawia Rysunek 1.



Rysunek 1 Schemat architektury systemu OpenAirInterface dla sieci 5G

Poszczególne elementy modułu OAI-5GC realizują wybrane funkcje wirtualne sieci szkieletowej w architekturze systemu 5G. Są to następujące funkcje:

AMF (ang. *Access and Mobility Management Function*):

Funkcja zarządza dostępem i mobilnością użytkowników w sieci 5G, ustanawia i kontroluje sesje użytkowników oraz zarządza mechanizmem przełączania (handover), odpowiada za autoryzację i uwierzytelnienie użytkowników.

SMF (ang. *Session Management Function*):

Funkcja zarządza sesjami użytkowników i przypisuje im odpowiednie usługi sieciowe, kontroluje i zarządza ruchem danych użytkowników, w tym QoS (ang. *Quality of Service*).

UPF (ang. *User Plane Function*):

Funkcja obsługuje ruch użytkowników i zarządza przepływem danych, odpowiada za ruch pakietowy, realizuje komutację pakietów (packet switching). Jest odpowiedzialna za rozróżnianie ruchu na różnych poziomach QoS.

AUSF (ang. *Authentication Server Function*):

Funkcja odpowiada za autoryzację i uwierzytelnienie użytkowników 5G w oparciu o protokół AKA (ang. *Authentication and Key Agreement*).

NRF (ang. *Network Repository Function*):

Funkcja przechowuje informacje o dostępnych funkcjach sieciowych (ang. *Network Functions* - NFs) w sieci 5G. Umożliwia dynamiczne wybieranie funkcji w zależności od potrzeb.

UDM (ang. *Unified Data Management*):

Funkcja zarządza danymi użytkowników, w tym profilami usług i subskrypcjami.

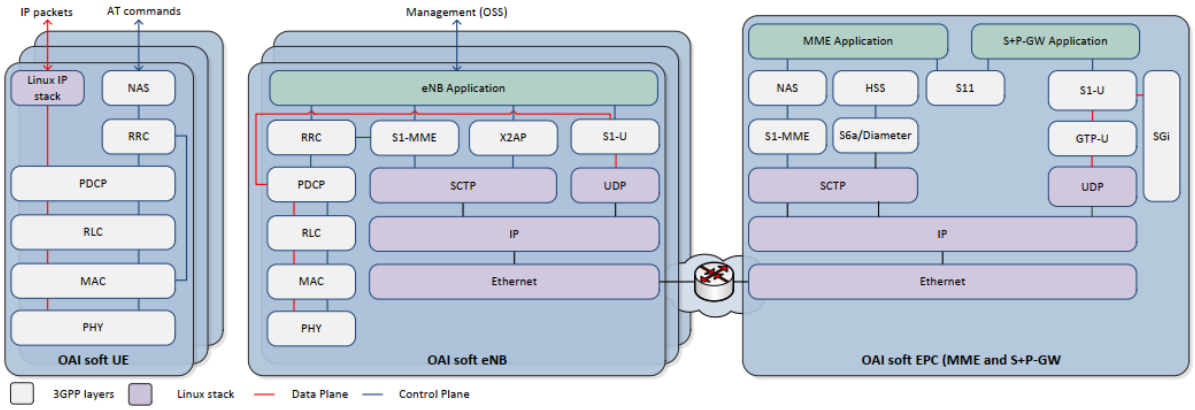
PCF (ang. *Policy Control Function*):

Funkcja zarządza politykami sieciowymi i QoS dla użytkowników 5G, umożliwia kontrolę nad jakością i priorytetem usług w sieci.

Moduł OAI-5GC może być zrealizowany na maszynach wirtualnych (ang. *Virtual Machines* - VMs) lub fizycznych maszynach, działających na systemie operacyjnym Linux. Konfiguracja modułu OAI-5GC obejmuje ustalenie parametrów sieciowych, adresów IP, adresów portów i interfejsów komunikacyjnych między komponentami. Interfejsy takie jak np. NGAP (ang. *Next Generation - Application Protocol*) służą do komunikacji między AMF, SMF a gNodeB (OAI-gNB). W ramach sieci szkieletowej istnieje możliwość skalowania i tworzenia klastrów dla poprawy wydajności i niezawodności sieci. Moduł OAI-5GC realizuje także wsparcie dla redundantnych konfiguracji w celu zapewnienia dostępności emulowanych usług systemu 5G.

Moduł OAI-gNB (gNodeB) działa jako stacja bazowa systemu 5G, obsługując interfejs radiowy NR i komunikację z modułem OAI-UE. W ramach modułu OAI-gNB realizowane jest zarządza zasobami radiowymi w taki sposób by zapewnić jakość połączeń na odpowiednim poziomie QoS.

Realizacja modułu OAI-gNB (OpenAirInterface gNodeB) obejmuje stworzenie i konfigurację stacji bazowej 5G, która jest kluczowym elementem w architekturze sieci dostępowej systemu komórkowego. Wspomniany moduł realizuje protokoły należące do poszczególnych warstw z modelu sieciowego OSI. Rysunek 2 przedstawia poszczególne elementy stosu protokołów sieci LTE realizowane przez system OAI. Pokazano na nim główne warstwy i funkcje realizowane przez narzędzie OAI oraz zilustrowano jak dane przepływają od aplikacji użytkownika do warstwy fizycznej, gdzie są transmitowane do sieci dostępowej. Implementacja OAI umożliwia testowanie i symulowanie różnych scenariuszy użytkowania w sieciach 5G, wspierając rozwój i wdrażanie nowych rozwiązań.



Rysunek 2 Elementy stosu protokołów sieci LTE realizowane przez system OAI [14].

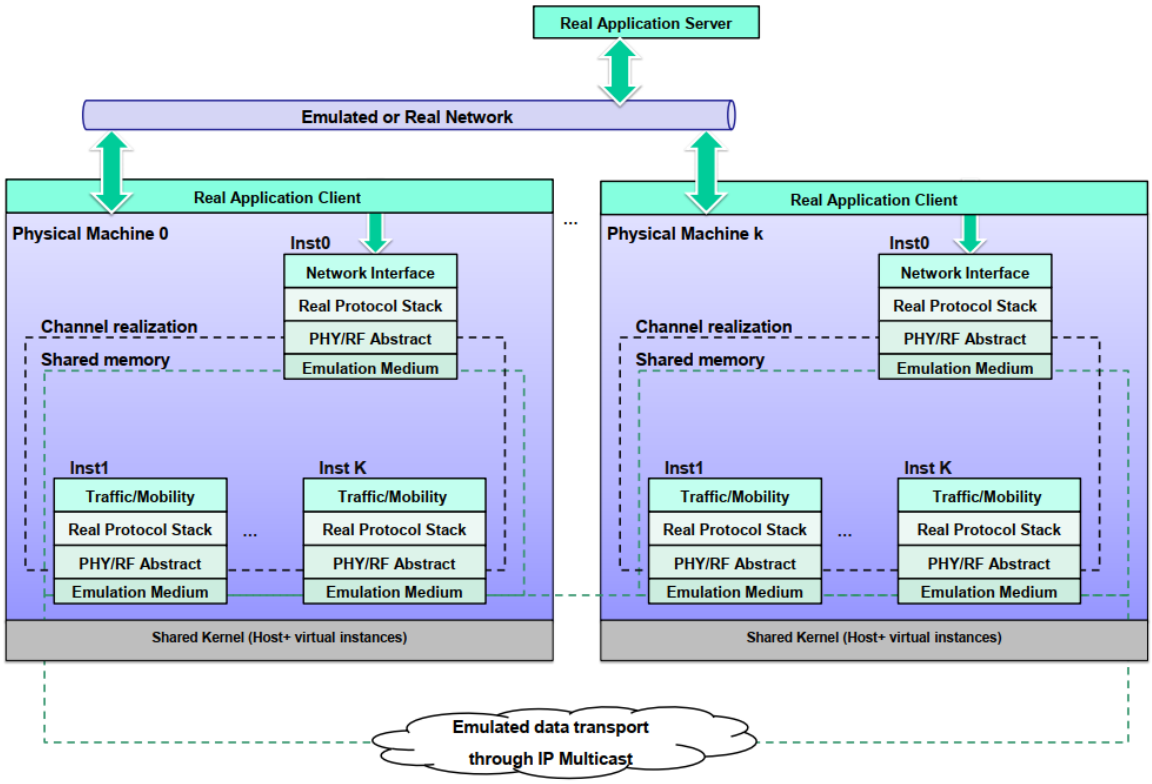
Są to warstwa fizyczna (PHY), warstwa łącza danych (MAC), warstwa kontroli łącza radiowego (RLC), warstwa sterowania zasobami radiowymi (RRC), wybrane interfejsy kontrolne. Warstwa PHY odpowiada za przetwarzanie sygnałów radiowych. W jej ramach realizowane są operacje modulacji i demodulacji, multipleksowanie, kodowanie i dekodowanie sygnałów. Warstwa MAC zarządza dostępem do medium radiowego oraz realizuje transmisję zgodnie z wielodostępem OFDMA (ang. *Orthogonal Frequency-Division Multiple Access*). Kontroluje dostęp do zasobów radiowych i nadzoruje transmisje do i od poszczególnych użytkowników pracujących w ramach poszczególnych stacji bazowych. Warstwa RLC zapewnia niezawodność transmisji danych. Dzieli dane na pakiety, zarządza ich kolejkowaniem i odbiorem. Warstwa RRC zarządza połączeniami i mobilnością poszczególnych użytkowników. Ustanawia i kontroluje sesje użytkowników w sieci. Spośród interfejsów realizowany jest interfejs kontrolny NG-ENB (Next Generation - eNodeB) Interface. Jest to interfejs łączący OAI-gNB z 5G Core (OAI-5GC), umożliwiający zarządzanie i kontrolę nad połączeniami użytkowników oraz przepływem danych w płaszczyźnie użytkownika. Interfejs X2 łączący stacje bazowe gNodeB, używany m.in. do zarządzania mechanizmem handover i koordynacji między stacjami bazowymi.

Moduł OAI-gNB może być zrealizowany przy użyciu platformy sprzętowej kompatybilnej z platformą USRP (ang. *Universal Software Radio Peripheral*). Wymaga odpowiedniej anteny, wzmacniacza i innych urządzeń służących do transmisji i odbioru sygnałów radiowych. Instalacja i konfiguracja oprogramowania OpenAirInterface (OAI) wymaga odpowiedniego systemu operacyjnego. Może to być np. system Linux. Konfiguracja modułu wymaga stworzenia plików konfiguracyjnych dla gNodeB (gnb.conf), określających m.in. parametry radiowe, IP i porty interfejsów kontrolnych.

Moduł OAI-UE (User Equipment) symuluje pracę urządzeń użytkownika sieci 5G, takich jak smartfony lub modemy. Podstawowe funkcje tego modułu to nawiązywanie połączeń z OAI-gNB i komunikacja z modułem sieci szkieletowej 5G Core poprzez stację bazową. Realizacja modułu OAI-UE (ang. *OpenAirInterface User Equipment*) jest kluczowa z punktu widzenia symulowania i testowania nowych funkcji urządzeń użytkowników działających w ramach sieci 5G.

Moduł OAI-UE może być realizowany na komputerach z systemem operacyjnym Linux. Może działać na różnych platformach sprzętowych kompatybilnych z SDR (Software-Defined Radio), takich jak USRP (ang. *Universal Software Radio Peripheral*). Konfiguracja modułu OAI-UE obejmuje ustalenie parametrów sieciowych, adresów IP, portów i interfejsów komunikacyjnych. Konfiguracja plików ue.conf, które definiują parametry połączenia i ustawienia warstwy fizycznej. Istnieje możliwość uruchamiania wielu instancji OAI-UE w celu symulacji działania urządzeń końcowych wielu użytkowników. Za pomocą wspomnianego modułu można testować funkcje urządzenia końcowego pracującego w różnych trybach, np. podczas realizacji mechanizmu handover, czy zmiany stanu urządzenia.

Narzędzie OAI bazuje na generatorze zdarzeń dyskretnych, emuluje działanie poszczególnych fragmentów sieci 5G poprzez przekazywanie informacji między funkcjami realizującymi kolejne protokoły systemu komórkowego. Przepływ informacji między poszczególnymi fragmentami oprogramowania OAI został przedstawiony na Rysunek 3.



Rysunek 3 Przepływ informacji między poszczególnymi fragmentami oprogramowania OAI realizującymi kolejne protokoły systemu 5G [16].

3.2 SRSRAN

Projekt srsRAN tworzony jest na zasadach licencji open source przez firmę Software Radio Systems Limited (SRS). W ramach projektu udostępniane jest oprogramowanie realizujące funkcje sieci dostępowej telefonii komórkowej 4 i 5 generacji o nazwie srsRAN. Narzędzie srsRAN jest całościowym rozwiązaniem dostępowej sieci radiowej systemu 5G zbudowanym zgodne ze specyfikacjami 3GPP i stowarzyszenia O-RAN Alliance. Narzędzie srsRAN realizuje większość protokołów warstwy pierwszej, drugiej i trzeciej. Oprogramowanie jest przenośne między architekturami procesorów i skalowalne. Może być uruchamiane zarówno na systemach wbudowanych o niskim poborze mocy jak i na systemach wykorzystujących zasoby w chmurze obliczeniowej. Narzędzie to stanowi platformę do badań i rozwoju mobilnych rozwiązań bezprzewodowych. Oprogramowanie srsRAN może być używane do przeprowadzania symulacji różnych scenariuszy obciążenia sieci komórkowej oraz analizy wydajności różnych konfiguracji sieciowych. Przy jego pomocy można testować nowe algorytmy związane z transmisją danych, zarządzaniem zasobami radiowymi czy optymalizacją sieci. Badacze mogą używać srsRAN do analizy i testowania zabezpieczeń w sieciach LTE i 5G, identyfikując potencjalne luki i proponując skuteczne rozwiązania.

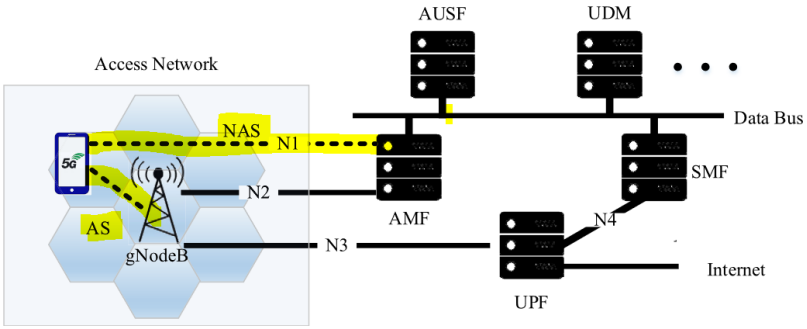
Narzędzie umożliwia szybką implementację prototypów i testowanie nowych rozwiązań w zakresie sieci bezprzewodowych, co jest niezwykle cenne dla firm technologicznych i startupów. Oprogramowanie srsRAN jest szeroko stosowanym narzędziem w uniwersytetach i instytucjach badawczych do prowadzenia badań nad sieciami komórkowymi. Służy do analizy wydajności oraz testowaniem nowych protokołów i technologii. Może być używane na różnych platformach, w tym na systemie Linux. Jest kompatybilne z urządzeniami USRP, co pozwala na wykorzystanie taniego sprzętu radiowego do budowy i testowania sieci LTE i 5G. Architektura srsRAN jest zaprojektowana tak, aby zapewnić elastyczność, modułowość i skalowalność w badaniach i rozwoju sieci komórkowych. Składa się z kilku kluczowych komponentów, które razem tworzą kompletny stos LTE/5G. Składa się z modułu sieci szkieletowej srsEPC (ang. *Evolved Packet Core*)/srs5GC, modułu sieci dostępowej srsENB (ang. *Evolved Node B*)/srsRAN 5G NR oraz modułu wyposażenia użytkownika srsUE (ang. *User Equipment*)**.**

W skład sieci szkieletowej srsEPC (Evolved Packet Core) wchodzą komponenty takie jak MME (ang. *Mobility Management Entity*), SGW (ang. *Serving Gateway*) i PGW (ang. *Packet Data Network Gateway*), które zarządzają mobilnością użytkowników, autoryzacją użytkowników, routowaniem pakietów i połączeniami z siecią zewnętrzną.

Element srsENB (ang. *Evolved Node B*) obsługuje wszystkie niezbędne funkcje stacji bazowej, w tym zarządzanie zasobami radiowymi, planowanie przydziałów zasobów radiowych, obsługę warstwy MAC (ang. *Medium Access Control*) i RLC (ang. *Radio Link Control*). Umożliwia budowanie stacji bazowej LTE do celów badawczych, testowania i implementacji prototypów.

Część srsUE (ang. *User Equipment*) symuluje działanie telefonu komórkowego, obsługując wszystkie niezbędne warstwy protokołów, w tym warstwę fizyczną PHY (ang. *Physical Layer*), warstwę dostępu do łącza MAC, kontroler łącza radiowego RLC, protokół PDCP (ang. *Packet Data Convergence Protocol*), kontroler ruchu radiowego RRC (ang. *Radio Resource Control*) i protokołów NAS (ang. *Non-Access Stratum*). Protokoły NAS to warstwa protokołów w architekturze sieci komórkowych, która działa powyżej warstwy dostępowej AS (ang. *Access Stratum*). Warstwa NAS jest odpowiedzialna za zarządzanie połączeniami i mobilnością oraz za przesyłanie wiadomości sygnalizacyjnych między urządzeniem użytkownika (ang. *User Equipment*, UE) a rdzeniem sieci (ang. *Core Network*). Warstwa NAS obsługuje procedury związane z mobilnością, takie jak rejestracja w sieci, autoryzacja, przydzielanie identyfikatorów oraz śledzenie lokalizacji użytkownika. W LTE jest to

obsługiwane przez Mobility Management Entity (MME), natomiast w 5G NR przez Access and Mobility Management Function (AMF). Warstwa ta kontroluje nawiązywanie, utrzymanie i zakończenie połączeń użytkownika. Obejmuje to zarządzanie sesjami, w tym inicjowanie połączeń danych oraz zarządzanie jakością usług (ang. *Quality of Service*, QoS). Warstwa NAS odpowiada za zarządzanie kluczami bezpieczeństwa i procedurami szyfrowania, aby zapewnić bezpieczną komunikację między UE a siecią. Zawiera mechanizmy autoryzacji i uwierzytelnienia użytkowników. Zarządza sesjami danych, w tym ustanawianiem, modyfikowaniem i usuwaniem sesji danych pakietowych, które są realizowane przez Serving Gateway (SGW) i Packet Data Network Gateway (PGW) w LTE oraz przez Session Management Function (SMF) w 5G NR. Warstwa NAS obejmuje kilka protokołów i wiadomości, które są przesyłane między UE a rdzeniem sieci. Główne komponenty NAS to m.in. procedury Attach, Detach Procedure, Authentication Request, Tracking Area Update, Service Request, Security Mode Command**,** Paging. Attach Procedure jest procedurą dołączenia urządzenia do sieci, obejmująca identyfikację i autoryzację użytkownika. Stanowi ona żądanie wysyłane przez UE do MME (w LTE) lub AMF (w 5G NR) w celu dołączenia do sieci. Żądanie Authentication Request jest przesyłane między siecią szkieletową a UE w celu przeprowadzenia procedur autoryzacji. Procedura Detach Procedure realizuje odłączanie urządzenia od sieci. Tracking Area Update (TAU) aktualizuje lokalizację użytkownika, gdy przemieszcza się on między obszarami zasięgu. Jest to informacja wysyłana przez UE do MME/AMF w celu zaktualizowania lokalizacji UE w sieci. Service Request realizuje żądanie usługi, inicjowane przez UE w celu nawiązania połączenia danych. Security Mode Command jest poleceniem służącym do ustawienia trybów bezpieczeństwa dla komunikacji między UE a siecią. Z kolei Paging jest mechanizmem, który umożliwia sieci powiadamianie UE o przychodzących połączeniach lub wiadomościach. Warstwy AS (ang. *Access Stratum*) oraz NAS (ang. *Non-Access Stratum*) zostały zaznaczone w schemacie architektury sieci 5G na Rysunek 4.

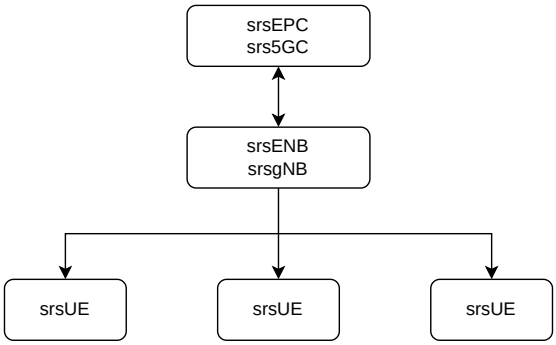


Rysunek 4 Umiejscowienie warstw AS (Access Stratum) oraz NAS (Non-Access Stratum) w architekturze sieci 5G [2]

Opisując warstwę NAS warto wspomnieć, że warstwa Access Stratum (AS) to warstwa odpowiedzialna za bezpośrednią komunikację radiową między UE a stacją bazową (eNodeB w LTE lub gNodeB w 5G NR). Obejmuje warstwę fizyczną PHY, MAC, RLC i PDCP. Warstwa AS zajmuje się zarządzaniem zasobami radiowymi, kontrolą dostępu i transportem danych użytkownika. Opisana wcześniej warstwa NAS działa powyżej AS i nie jest bezpośrednio zaangażowana w transport danych radiowych. Zamiast tego, zajmuje się zarządzaniem połączeniami, mobilnością i bezpieczeństwem. Część oprogramowania srsRAN 5G NR realizuje techniki wykorzystywane w standardzie 5G, w tym modulację OFDM, technikę MIMO, zarządzanie zasobami i planowaniem zasobami dla sieci 5G NR.

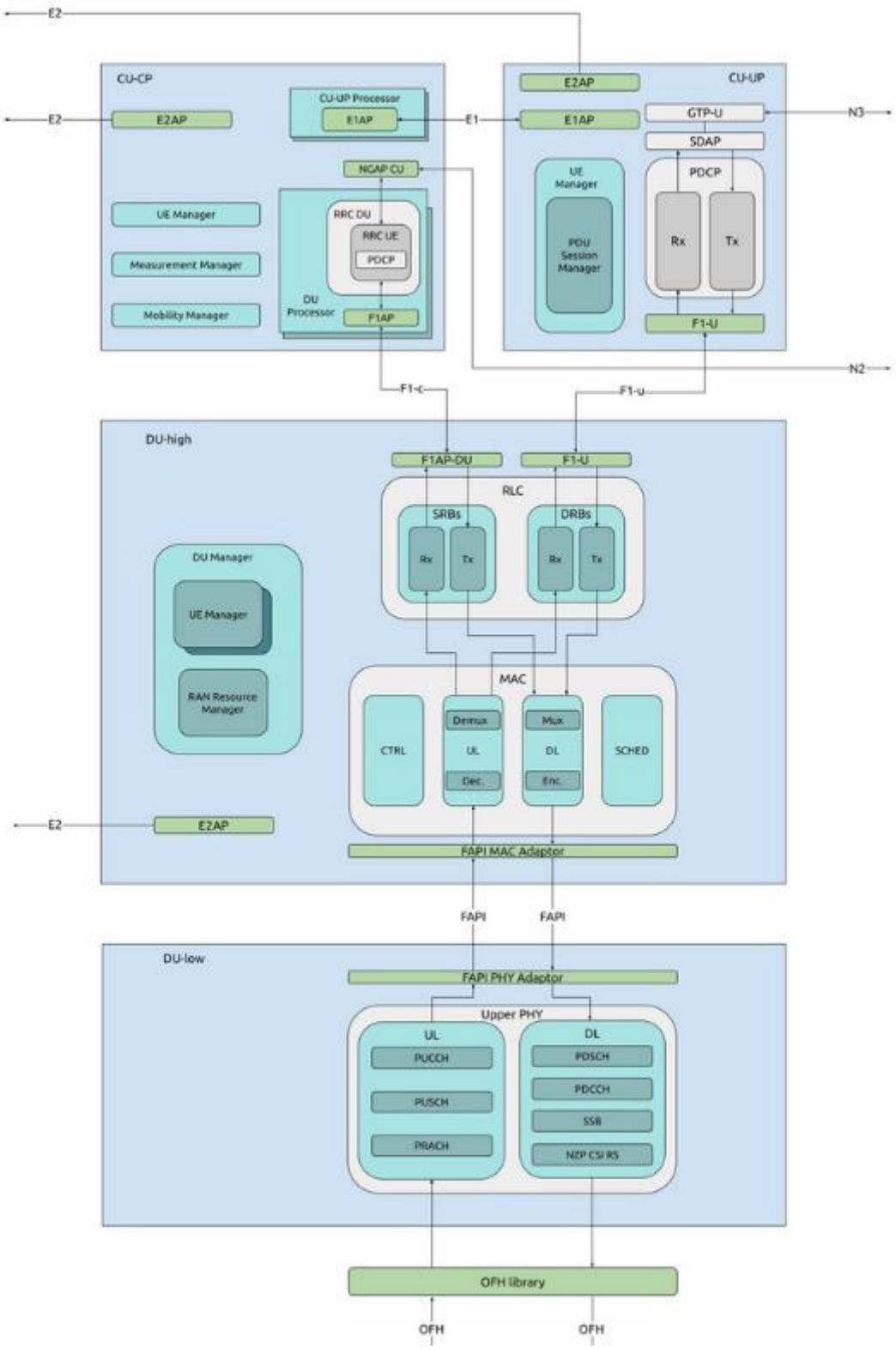
Architektura srsRAN jest zaprojektowana w sposób modułowy. Pozwala to na łatwe dodawanie, usuwanie lub modyfikowanie poszczególnych komponentów. Każdy komponent stanowi oddzielną procedurę programową. Działa ona jako osobny moduł, który można niezależnie rozwijać i testować. Oprogramowanie srsRAN można skalować w zależności od potrzeb badawczych lub testowych, od pojedynczych węzłów do rozbudowanych sieci z wieloma stacjami bazowymi i użytkownikami. Moduł srsRAN obsługuje interfejsy radiowe zgodne ze standardami LTE i 5G, umożliwiając komunikację z komercyjnymi urządzeniami użytkownika oraz innymi stacjami bazowymi. Z kolei moduł srsEPC zapewnia interfejsy sieciowe do komunikacji z sieciami zewnętrznymi, w tym Internetem, umożliwiając pełne testowanie połaczeń end-to-end.

Narzędzie srsRAN jest zaprojektowane do współpracy z urządzeniami USRP, które są popularnymi platformami sprzętowymi do badań nad sieciami radiowymi. Urządzenia USRP umożliwiają transmisję i odbiór sygnałów radiowych, co jest kluczowe dla testowania i prototypowania sieci LTE/5G w rzeczywistych warunkach. Na rysunku 5 przedstawiono schemat architektury narzędzia srsRAN uwzględniający kluczowe komponenty i ich wzajemne powiązania.



Rysunek 5 Schemat architektury narzędzia srsRAN emulującego działanie sieci 5G.

W powyższym schemacie, moduł sieci szkieletowej srsEPC zarządza połączeniami i routingiem danych, moduł srsENB działa jako stacja bazowa, a moduł srsUE symuluje urządzenia użytkownika. Wszystkie te komponenty mogą komunikować się za pośrednictwem interfejsów radiowych i sieciowych. Architektura srsRAN (5G) została zaprojektowana, aby wspierać rozwój i badania nad nowoczesnymi sieciami 5G NR (New Radio). Na stronie projektu srsRAN [9] został przedstawiony szczegółowy schemat architektury oprogramowania srsRAN realizującego poszczególne funkcjonalności stacji bazowej systemu 5G, Rysunek 6. Poszczególne komponenty oprogramowania srsRAN (5G) realizują funkcje stacji bazowej srsGNB (gNodeB), sieci szkieletowej srs5GC (5G Core) oraz wyposażenia/urządzenia użytkownika srsUE (User Equipment). Moduł stacji bazowej srsGNB (gNodeB) obsługuje interfejs radiowy 5G NR, zarządza zasobami radiowymi oraz obsługuje połączenia z urządzeniami użytkownika (UE). W module tym implementowane są również elementy warstwy fizycznej, warstwy dostępu do medium transmisyjnego (Medium Access Control - MAC), warstwy kontroli łącza radiowego (Radio Link Control RLC), szyfrowanie realizowane w warstwie PDCP (Packet Data Convergence Protocol) oraz zarządzenie zasobami radiowymi w module sterującym zasobami radiowymi RRC (Radio Resource Control) [3].



Rysunek 6 Schemat architektury oprogramowania srsRAN realizującego funkcjonalności stacji bazowej sieci 5G [4]

W module sieci szkieletowej realizowane są następujące funkcjonalności: zarządzanie dostępem i mobilnością użytkowników w ramach funkcji AMF (Access and Mobility

Management Function), zarządzanie sesjami danych w ramach funkcji SMF (Session Management Function), przetwarzanie danych użytkowników realizowane przez funkcję UPF (User Plane Function), a także zarządzanie politykami sieci – funkcja PCF (Policy Control Function), oraz uwierzytelnianie użytkowników realizowane przez funkcję AUSF (Authentication Server Function). Moduły srsUE symulują działanie terminali 5G obsługując wszystkie niezbędne warstwy protokołów.

Narzędzie srsRAN realizuje połączenie i autoryzację użytkownika wg następującego scenariusza. Moduł srsUE wysyła żądanie połączenia do modułu srsgNB, który je przekazuje do funkcji AMF znajdującej się w module sieci szkieletowej srs5GC. Funkcja AMF realizuje autoryzację użytkownika, czyli modułu srsUE i inicjuje ustanowienie sesji. Po ustanowieniu sesji, dane użytkownika przenoszone są przez moduł srsgNB do funkcji UPF. Funkcja ta następnie przesyła dane do odpowiednich funkcji sieciowych lub zewnętrznych sieci IP. Z kolei funkcja AMF zarządza mobilnością, steruje mechanizmem handover. Jeśli zakładamy, że użytkownik się przemieszcza to następuje przełączanie modułu srsUE między różnymi modułami srsgNB. Funkcja UPF przełącza dane między odpowiednimi modułami srsgNB, zapewniając ciągłość realizowanego połączenia

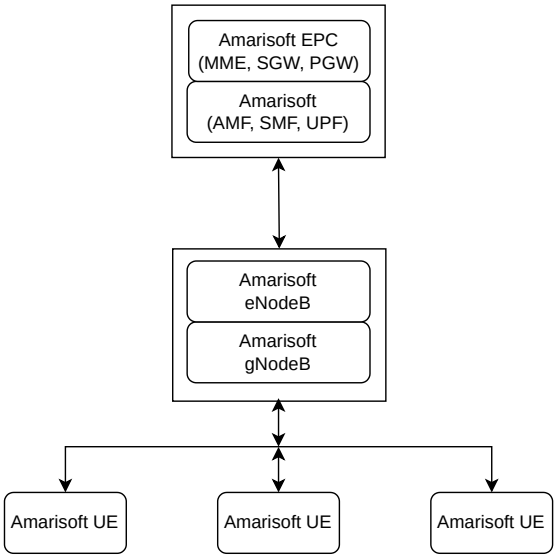
W ramach narzędzia srsRAN realizowane są również odpowiednie interfejsy 3GPP sieci 5G. Interfejs NG łączy moduł srsGNB z funkcjami AMF i UPF realizowanymi w ramach sieci szkieletowej, czyli modułu srs5GC. Interfejs N3 łączy funkcję UPF ze stacją bazową srsgNB. Interfejs N4 łączący funkcję SMF z funkcją UPF. Interfejs N6 łączący funkcję UPF z zewnętrznymi sieciami pakietowymi IP.

3.3 AMARISOFT

Firma Amarisoft oferuje komercyjne oprogramowanie AMARI Callbox do budowy i testowania sieci komórkowych, w tym LTE i 5G [12]. Oprogramowanie Amarisoft charakteryzuje się dużą elastycznością i skalowalnością, co czyni go popularnym narzędziem wśród operatorów sieci, producentów sprzętu i instytucji badawczych. AMARI Callbox jest rozwiązaniem, które łączy w sobie funkcje stacji bazowej sieci szkieletowej oraz wyposażenia użytkownika. Dzięki temu możliwe jest testowanie różnych aspektów funkcjonowania sieci komórkowych od mechanizmów rejestracji urządzeń końcowych w sieci poprzez funkcje zarządzania połączeniami, przesyłaniem informacji w płaszczyźnie użytkownika po realizację testów wydajnościowych i optymalizacyjnych sieci komórkowej. Kluczowe komponenty

AMARI Callbox stanowią moduły realizujące funkcje stacji bazowej Amarisoft LTE eNB oraz 5G gNB. Moduł stacji bazowej realizuje funkcje warstwy fizycznej, MAC, RLC, PDCP, RRC i pozostałych warstw niezbędnych do działania stacji bazowej. Obsługuje zarządzanie zasobami radiowymi, zarządzanie połączeniami oraz przekazywanie danych użytkowników. Oferuje pełną funkcjonalność warstwy fizycznej i wyższych warstw sieci 5G. W module tym realizowane są m.in. algorytmy modulacji, kodowania, zarządzania zasobami radiowymi, sterowania transmisją wieloantenową MIMO.

Na Rysunek 7 przedstawiono schemat architektury narzędzia AMARI Callbox uwzględniający kluczowe moduły i ich wzajemne powiązania.

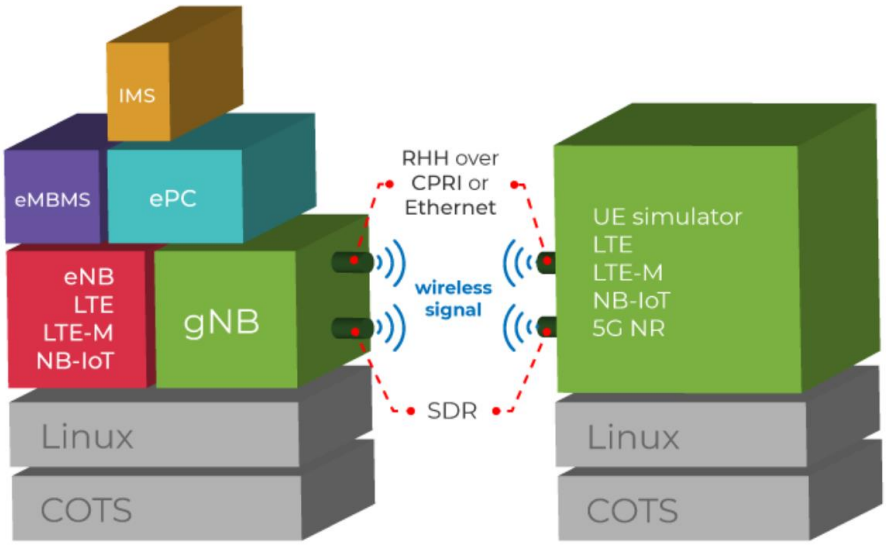


Rysunek 7 Schemat architektury AMARI Callbox uwzględniający podstawowe moduły

AMARI Callbox zawiera w swojej strukturze moduły sieci szkieletowej LTE Amarisoft EPC (ang. Evolved Packet Core) i sieci 5G Amarisoft 5GC (ang. 5G Core Network). Moduł sieci szkieletowej realizuje funkcjonalności jednostki zarządzania mobilnością MME, serwerów SGW i PGW, bazy danych HSS, które odpowiadają odpowiednio za realizację zarządzania mobilnością, routingiem danych pakietowych, autoryzacją użytkowników. Moduł ten obejmuje także komponenty funkcji wirtualnych AMF, SMF, UPF, PCF, UDM, które zarządzają sesjami, mobilnością, routingiem danych oraz funkcjami kontroli i polityki bezpieczeństwa w sieci 5G. Najmniej złożony jest moduł Amarisoft UE (User Equipment), który emuluje działanie urządzenia końcowego, obsługując pełen zestaw protokołów od warstwy fizycznej po aplikacyjną.

Oprogramowanie firmy Amarisoft współpracuje z różnymi platformami SDR (Software-Defined Radio). Umożliwia to realizację w elastyczny sposób transmisji i odbioru sygnałów radiowych stosowanych w telefonii komórkowej LTE i 5G. Typowymi platformami SDR używanymi z Amarisoft są produkty Ettus Research, np. USRP. Oprogramowanie Amarisoft jest w pełni zgodne z odpowiednimi standardami 3GPP dla LTE i 5G NR. Implementuje protokoły warstwy fizycznej (PHY), dostępu do medium - MAC, RLC, PDCP, RRC oraz NAS. Komponenty sieci szkieletowej LTE i 5G zarządzają połączeniami, mobilnością, bezpieczeństwem i sesjami danych. Realizują interfejsy do zarządzania, monitorowania i konfiguracji sieci LTE i 5G.

Symulator sieci 5G AMARI Callbox umożliwia symulację protokołów występujących w sieci szkieletowej, stacjach bazowych gNodeB oraz terminalach. Symulator może pracować zarówno z wykorzystaniem łączności realizowanej za pomocą kart dostępu radiowego np. USRP jak też poprzez symulator kanału radiowego łączności komórkowej. Ogólna koncepcja architektury symulatora została zaprezentowana na Rysunek 8.



Rysunek 8 Ogólna koncepcja architektury symulatora AMARI Callbox [5]

Niestety kod rozwiązania AMARI Callbox nie jest udostępniany na zasadach open-source, przez to ingerencja w kod źródłowy jest utrudniona i implementacje nowych funkcji przy jego zastosowaniu są niemożliwe. Producent oferuje wspomniane oprogramowanie w kilku wersjach m.in. Mini, Classic, Advanced i Ultimate różniących się od siebie przede wszystkim wykorzystywaną specyfikacją sprzętową. Ma to bezpośredni wpływ na możliwości uruchamianej na określonej platformie sprzętowej funkcjonalności stacji bazowej 5G - gNodeB. W zależności od wersji platformy sprzętowej urządzenia Amarisoft są sprzedawane z

różnymi zestawami akcesoriów zewnętrznych. AMARI Callbox Classic zawiera 5 testowych kart SIM oraz 12 elementów antenowych. Zestaw AMARI Callbox Advanced składa się z pięciu testowych kart SIM, czterech elementów RF combiner umożliwiających realizację toru transmisyjnego bez promieniowania radiowego, szesnastu połączeń kablowych RG405 SMA i czterech elementów antenowych. Wersje Classic i Advanced różnią się wydajnością procesora zastosowanego w kartach SDR odpowiedzialnych za generację i odbiór sygnału radiowego NR. W wersji Advanced zastosowano karty umożliwiające wykorzystanie kanałów radiowych o szerokości 100 MHz. Umożliwia to uzyskanie dużych wartości przepływności w kanale radiowym, a zarazem stwarza możliwości wykorzystania mechanizmów agregacji pasm w konfiguracji stacji bazowej gNodeB. Dzięki temu w wersji Advanced w porównaniu do Classic można realizować większy zbiór scenariuszy zakładających wykorzystanie zarówno sieci 5G, jak też LTE oraz trybu transmisji IoT. Dodatkowo, zestaw Advanced wyposażony jest w niezbędne akcesoria zewnętrzne umożliwiające realizację scenariuszy badawczych bez promieniowania RF w trybie dupleksu częstotliwościowego (FDD), czasowego (TDD) oraz z zestawem wieloantenowym MIMO 4x4.

3.4 AETHER

Aether [13] jest otwartą platformą stworzoną w 2021 roku przez ONF (Open Networking Foundation), która umożliwia zarządzanie sieciami prywatnymi w technologii 4G/5G oraz funkcjami edge computing (przetwarzania na brzegu sieci). Jest zaprojektowana z myślą o elastycznym i skalowalnym wdrażaniu sieci komórkowych dla przedsiębiorstw i społeczności, wspierając różnorodne przypadki użycia od przemysłu po rolnictwo. Aether składa się z kilku kluczowych komponentów, które razem tworzą kompletną platformę zarządzania:

- Aether Control Plane (Aether-CP) - centralny element platformy, który zarządza i kontroluje wszystkie aspekty sieci komórkowej, takie jak rejestracja użytkowników, zarządzanie zasobami i politykami QoS.
- Aether Edge Node (Aether-EN) - węzły brzegowe odpowiedzialne za przetwarzanie danych blisko źródła ich generowania. Wspierają aplikacje wymagające niskich opóźnień.
- Aether Data Plane (Aether-DP) - płaszczyzna danych, która przekierowuje ruch sieciowy między urządzeniami końcowymi a Internetem lub lokalnymi zasobami.

- Aether Orchestration - moduł odpowiedzialny za automatyzację wdrażania i zarządzania zasobami sieciowymi, zapewniający elastyczność i łatwość skalowania.
- Aether Portal - interfejs użytkownika do zarządzania i monitorowania sieci, oferujący narzędzia do zarządzania użytkownikami, zasobami i politykami.

Do zalet Aether można zaliczyć: elastyczność i skalowalność (umożliwia łatwe skalowanie sieci w zależności od potrzeb, co jest idealne dla dynamicznych środowisk przedsiębiorstw i społeczności), niskie opóźnienia (dzięki edge computing, Aether pozwala na przetwarzanie danych blisko ich źródła, co redukuje opóźnienia i zwiększa wydajność), otwarta architektura (jako projekt open-source, Aether zapewnia elastyczność i możliwość dostosowania do specyficznych potrzeb użytkowników), zarządzanie przez chmurę (centralne zarządzanie przez chmurę umożliwia łatwe wdrażanie i zarządzanie sieciami prywatnymi bez potrzeby inwestowania w drogą infrastrukturę). Przykładowe obszary, w których można wykorzystać Aether to Przemysł 4.0. W tym zastosowaniu, firmy produkcyjne mogą korzystać z Aether do zarządzania swoimi sieciami przemysłowymi, zapewniając niezawodną łączność i przetwarzanie danych w czasie rzeczywistym dla urządzeń IoT. Ciekawym zastosowaniem tego rozwiązania może być rolnictwo precyzyjne, w którym Aether może być używany do zarządzania sieciami IoT, które monitorują warunki glebowe, pogodowe i zdrowie roślin, wspierając decyzje rolników oparte na danych. Następnym obszarem wykorzystania Aether są inteligentne miasta. W miastach inteligentnych Aether może zarządzać sieciami komórkowymi dla różnych aplikacji, takich jak monitorowanie ruchu, zarządzanie odpadami i systemy bezpieczeństwa publicznego.

Proces instalacji i uruchamiania środowiska Aether jest szczegółowo przedstawiony i omówiony na stronie: https://docs.aetherproject.org/master/onramp/start.html.

3.5 OPEN5GS

Open5GS [14] to projekt typu open-source, który ma na celu stworzenie kompletnych implementacji systemów komórkowych 4G (Long Term Evolution) i 5G (no-standalone i standalone) w pełni zgodnych ze standardami 3GPP [6]. Jest przeznaczony dla badaczy, inżynierów i entuzjastów, którzy chcą eksperymentować i budować własne sieci komórkowe. Open5GS został stworzony w celu umożliwienia dostępu do technologii 4G i 5G na zasadach open-source. Projekt ten wspiera rozwój badań i innowacji w dziedzinie telekomunikacji, dając możliwość tworzenia prywatnych sieci komórkowych i testowania nowych rozwiązań bez

konieczności korzystania z drogich, komercyjnych systemów. Pierwsza wersja Open5GS została opublikowana w 2017 roku. Aktualna wersja tego narzędzia nosi numer 2.7.1.

Architektura Open5GS obejmuje różne komponenty sieci komórkowych 4G i 5G, które są zgodne ze standardami 3GPP. Główne komponenty to (rysunek 9):

- Komponenty sieci 4G (LTE):

  - MME (ang *Mobility Management Entity*): Zarządza mobilnością użytkowników i sesjami, odpowiedzialny za sygnalizację i kontrolę.

  - SGW (ang. *Serving Gateway*): Przekierowuje pakiety danych między eNodeB a PGW.

  - PGW (ang. *Packet Data Network Gateway*): Łączy sieć LTE z zewnętrznymi sieciami IP, zapewniając dostęp do Internetu i innych usług.

  - HSS (ang. *Home Subscriber Server*): Przechowuje informacje o subskrybentach, takie jak dane uwierzytelniające, profile abonentów i klucze szyfrowania.

  - PCRF (ang. *Policy and Charging Rules Function*): Zarządza politykami QoS (ang. *Quality of Service*) i zasobami sieciowymi.

- Komponenty sieci 5G:

  - AMF (ang. *Access and Mobility Management Function*): Odpowiada za zarządzanie mobilnością i autoryzację użytkowników.

  - SMF (ang. *Session Management Function*): Zarządza sesjami i kontrolą ruchu danych.

  - UPF (ang. *User Plane Function*): Przekierowuje pakiety danych w płaszczyźnie użytkownika.

  - NRF (ang. *Network Repository Function*): Umożliwia rejestrację i odkrywanie funkcji sieciowych.

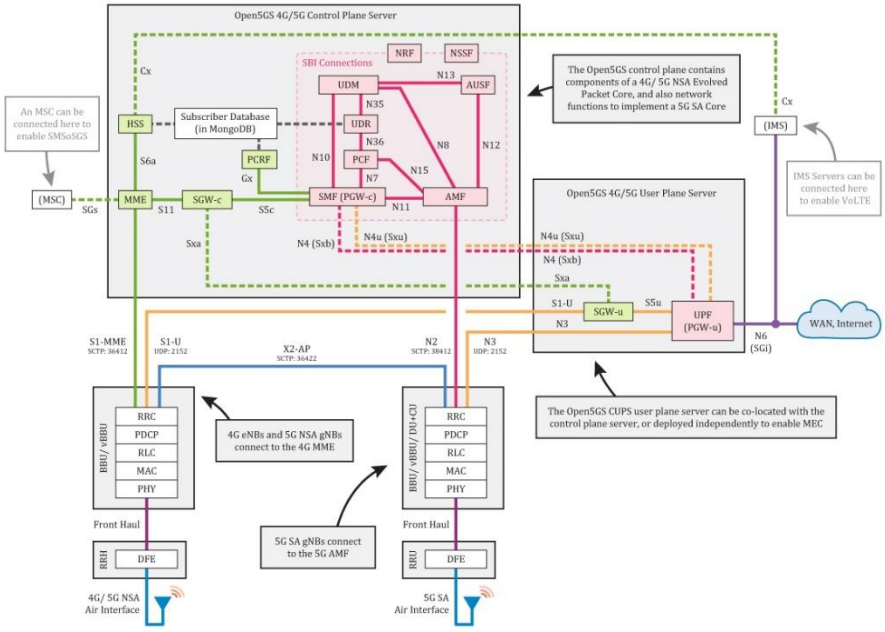
  - UDM (ang. *Unified Data Management*): Przechowuje dane abonentów i zarządza nimi.

  - PCF (ang. *Policy Control Function*): Zarządza politykami sieciowymi i zasobami.

Do zalet tego rozwiązania można zaliczyć: zgodność ze Standardami 3GPP [15] (co zapewnia interoperacyjność z innymi urządzeniami i systemami); modularność (dzięki

modularnej budowie, poszczególne komponenty mogą być wdrażane i konfigurowane niezależnie), skalowalność (możliwe jest budowanie sieci o dowolnych wielkościach od małych prywatnych sieci do większych implementacji komercyjnych) oraz elastyczność (możliwość dostosowania konfiguracji sieci do specyficznych potrzeb użytkownika).

Dzięki swoim zaletom Open5GS może być wykorzystywany w różnych obszarach takich jak badania i edukacja, gdzie w środowiskach akademickich i badawczych używany jest do eksperymentów z technologiami 4G i 5G oraz w procesie dydaktycznym. Również przemysł może korzystać z tego narzędzia jako platforma do testowania nowych rozwiązań, prototypowania i tworzenia prywatnych sieci komórkowych. Może być stosowany w sytuacjach kryzysowych do tworzenia tymczasowych sieci komunikacyjnych dla służb ratunkowych. W literaturze przedmiotu można znaleźć szereg artykułów, których autorzy w procesie prowadzonych badań wykorzystali Open5GS. Są to między innymi prace [16] i [17].

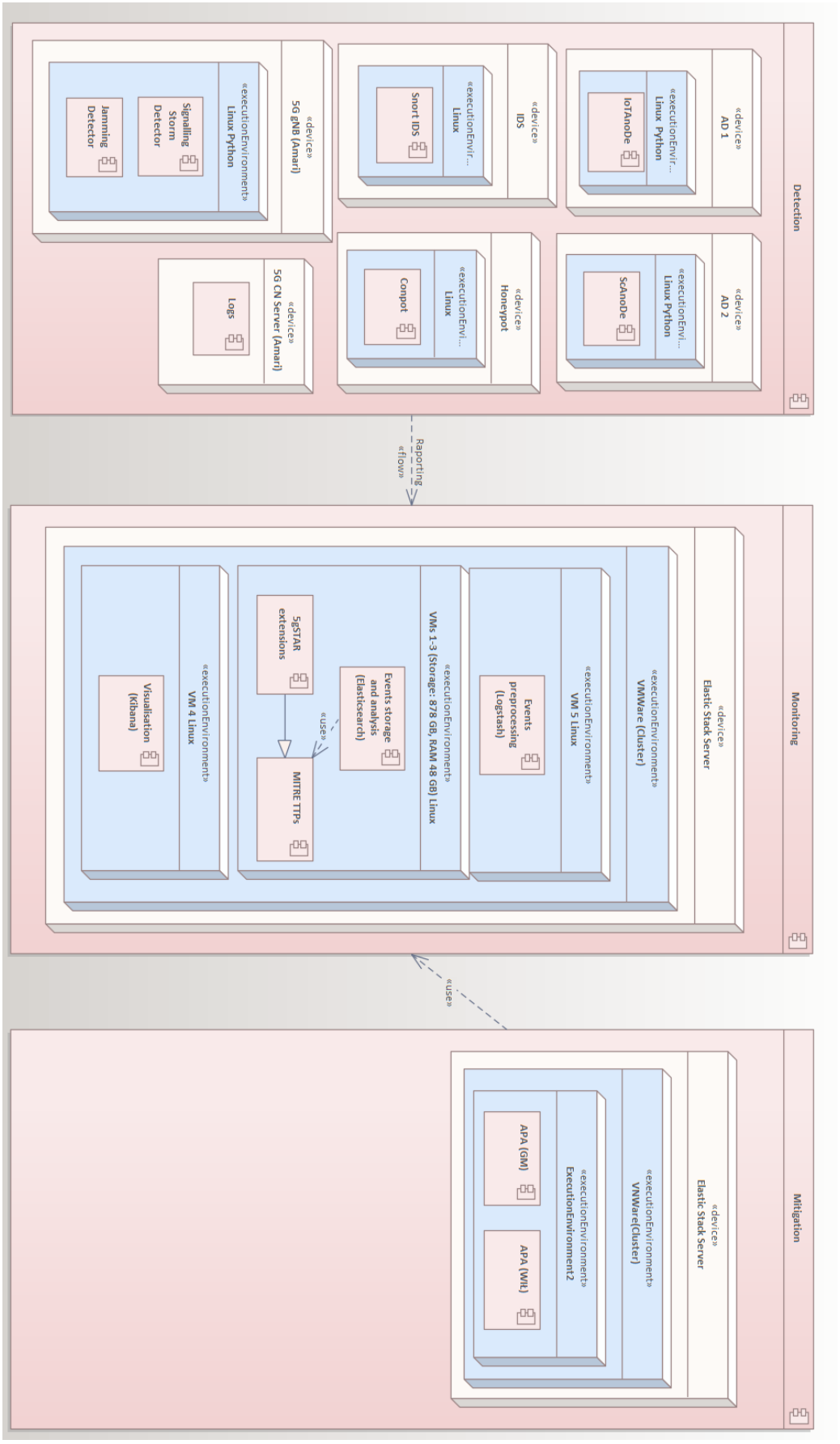


Rysunek 9 Budowa Open5GS [7]

4 PROJEKT OGÓLNY

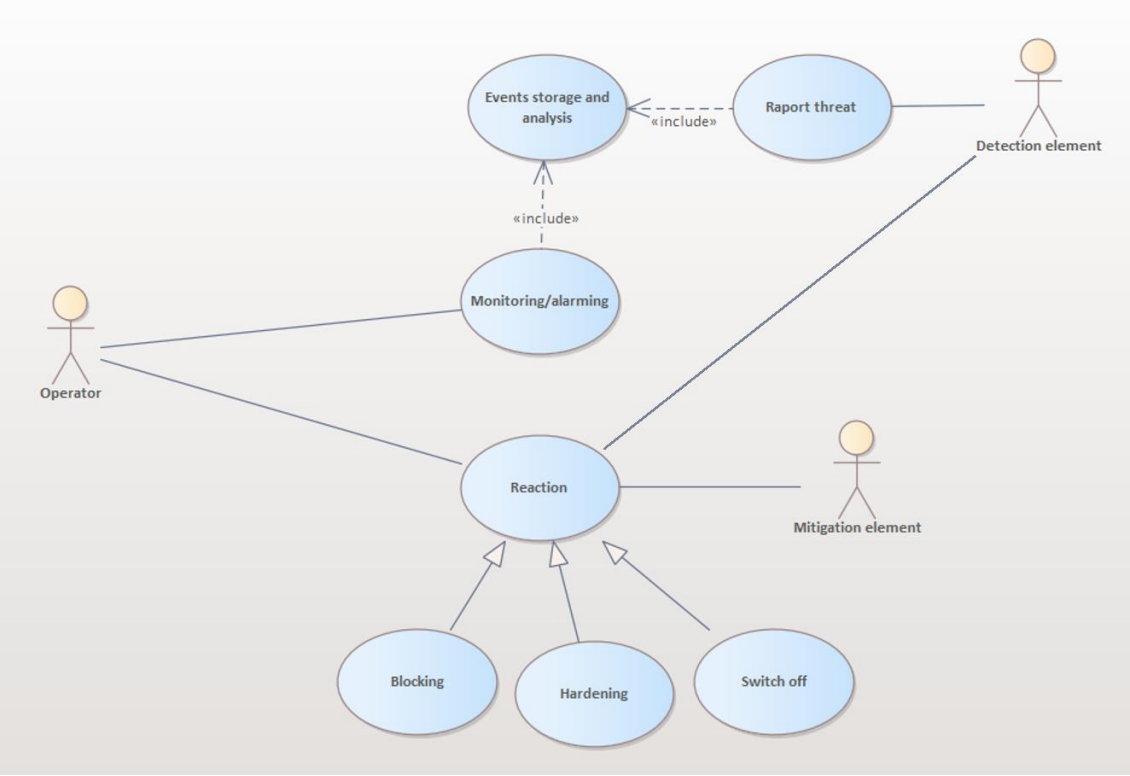
System 5gSTAR będzie zbudowany z komponentów podzielonych na obszary związane z detekcją, monitoringiem zagrożeń oraz mitygacją (reagowanie/działania zaradcze). Przekrój ogólny systemu 5gSTAR najlepiej obrazuje projekt w postaci diagramu UML wdrożenia przedstawiony na Rysunek 10. Przedstawiono na nim umiejscowienie elementów w zwirtualizowanym środowisku serwerowym opartym o rozwiązanie VMWare ESXi (www.vmware.com/products/esxi-and-esx.html). Wybrane oprogramowanie zarządcy wirtualizacji to tzw. *bare metal hyperivisor* klasy *enterprise* (natywny zarządca nie instalowany na dodatkowym systemie operacyjnym), które opiera się na własnym jądrze, konsoli serwisowej i własnych sterownikach. Ponieważ zarządca ma bezpośredni dostęp do sprzętu jest to rozwiązanie wysoce wydajne i skalowalne.

Detektory wykrywają zagrożenia w systemie, który monitorują i zgłaszają alerty o wykryciu ataku bądź jego symptomów do systemu monitorowania. System monitorowania składuje i przetwarza te dane, a następnie udostępnia informacje o zdarzeniu Operatorowi systemu poprzez dedykowaną konsolę (aplikację przeglądarkową opartą o rozwiązanie Kibana). Na bazie informacji o zagrożeniu, operator może podjąć akcje zaradcze (mitygacja) wykorzystując do tego celu dedykowane moduły APA (Aplikacja Przeciwdziałania Atakom). Jako platformę 5G wybrano rozwiązanie oparte o sieć rdzeniową Open5GS https://open5gs.org i stację bazową firmy Amarisoft (seria Amari Callbox Advance) https://www.amarisoft.com. UE (ang. *User Equipment*) stanowią elementy IIoT operte o modem firmy Simcom (https://simcom.com) na platformie Raspberry PI 4 (https://www.raspberrypi.org). Integracja z elementami nie wspierającymi komunikacji 5G będzie realizowana poprzez router 5G także oparty o modem firmy Simcom (https://simcom.com) na platformie Raspberry PI 4.



Rysunek 10 Projekt ogólny Systemu 5gSTAR w formie diagramu UML wdrożenia

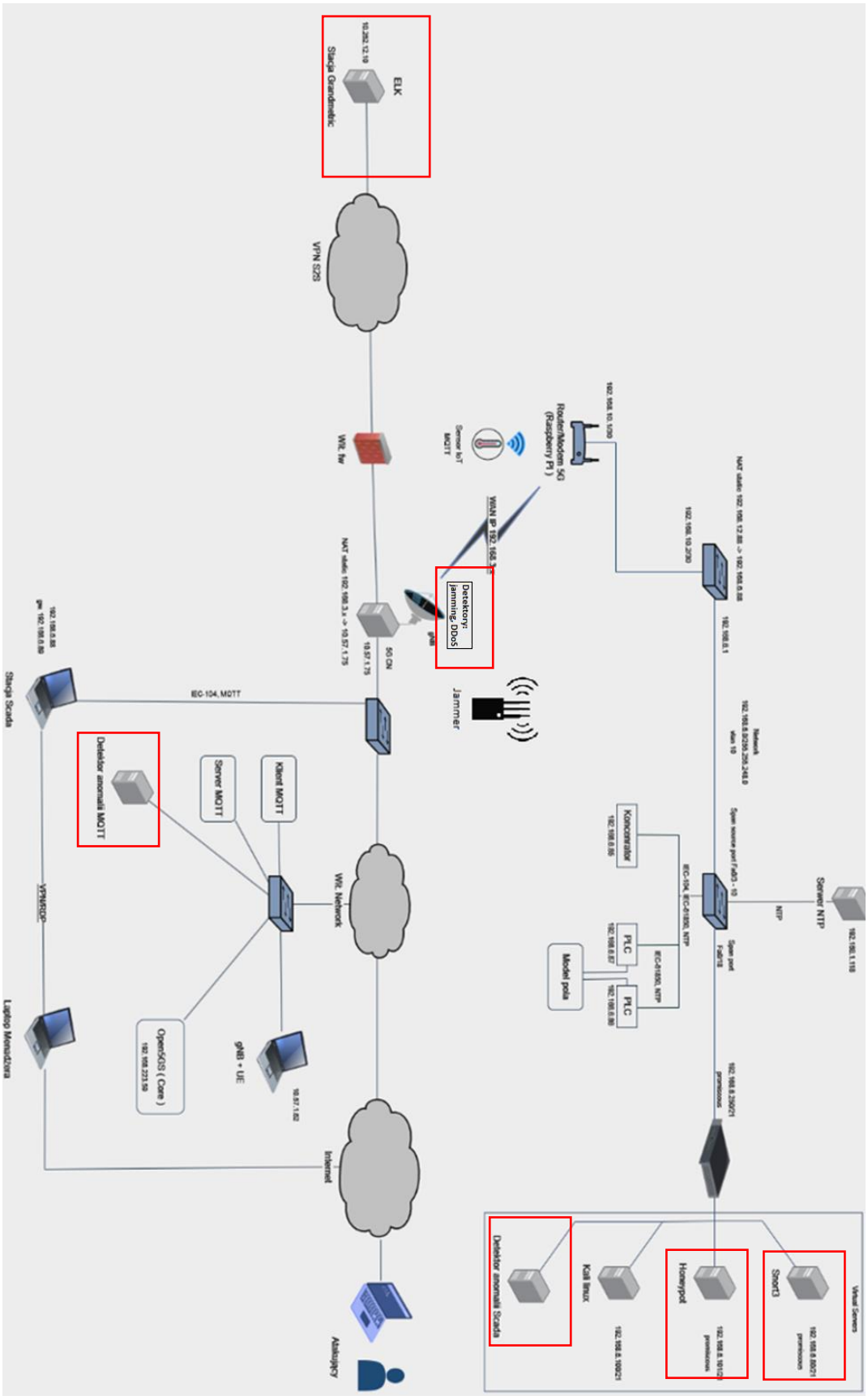
Diagram UML ogólnych przypadków użycia dla Systemu 5gSTAR przedstawiono na Rysunek 11.



Rysunek 11 Diagram UML ogólnych przypadków użycia Systemu 5gSTAR

Operator monitoruje nadzorowany system (np. sieć przemysłową wykorzystująca komunikacje 5G) za pomocą elementów Systemu 5gSTAR. Jego bezpośrednim interfejsem jest system monitorowania i reagowania udostępniony w formie przeglądarkowego interfejsu graficznego zrealizowanego w oparciu o narzędzie Kibana. Na podstawie alarmów o zaistniałych zagrożeniach zaraportowanych przez detektory, Operator podejmuje działanie zaradcze takie jak np.: wprowadzenie nowej (bardziej bezpiecznej) konfiguracji czasowe wyłączenie usługi/urządzenia czy blokowanie np. ruchu sieciowego. Należy zaznaczyć, że część detektorów (dla ataków typu *jamming* i *signalling storm*) ma posiadać funkcje automatycznego łagodzenia ataków.

Schemat utworzonego w Projekcie środowiska badawczego emulującego sieć przemysłową wykorzystującą 5G wraz z rozmieszczonymi elementami Systemu 5gSTAR (zaznaczonymi na czerwono) przedstawiono na Rysunek 12.



Rysunek 12 Umiejscowienie elementów Systemu 5gSTAR w środowisku badawczym opracowanym w Projekcie

W części przemysłowej środowisko badawcze bazuje na rzeczywistych urządzenia firmy Elkomtech, które emulują działanie stacji elektroenergetycznej dla linii średnich napięć zarządzanego poprzez SCADA. Monitoring i sterowanie elementami stacji elektroenergetycznej jest realizowane z wykorzystaniem protokołów sieciowych IEC-104 oraz IEC 61850. Podstawowymi elementami środowiska przemysłowego są: stacja SCADA (pełniącą funkcje *Human Machine Interface*), koncentrator, dwa sterowniki i model pola. Elementami uzupełniającymi środowisko przemysłowe są: ruter IP, przełącznik Ethernet, Stacja Inżynierska (komputer z systemem Linux przeznaczony do prac utrzymaniowych i diagnostycznych dla elementów SCADA) oraz serwer czasu NTP. Komunikacja pomiędzy sterownikami opiera się o protokół IEC 61850 GOOSE (rozgłoszenia realizowane na warstwie Ethernet). Komunikacja pomiędzy koncentratorem, a sterownikami jest oparta o protokół IEC 61850 MMS (stos Ethernet/IP/TCP, model klient-serwer). Komunikacja pomiędzy koncentratorem i stacją SCADA jest realizowana z wykorzystaniem protokołu IEC-104 (stos Ethernet/IP/TCP, model klient-serwer). Stacja SCADA znajduje się w chmurze (sieć Internet), a pozostałe elementy znajdują się w sieci NAT (ang. *Network Address Translation*), do której dostęp jest realizowany poprzez ruter brzegowy 5G łączący się ze stacją bazową 5G (gNB), która jest podłączoną do sieci rdzeniowej 5G (ang. CN, Core Network). Część 5G środowiska badawczego zrealizowano w oparciu o sieć rdzeniową Open5GS https://open5gs.org i stację bazową firmy Amarisoft (seria Amari Callbox Advance) https://www.amarisoft.com. Jako router 5G zastosowano modem firmy Simcom (https://simcom.com) na platformie Raspberry PI 4 (https://www.raspberrypi.org). W zaplanowanych w Projekcie scenariuszach sieć 5G jest zakłócana poprzez urządzenie zakłócające (ang. *jammer*). W środowisku umieszczono również element IoT 5G typu multisensor (kamera, czujniki: ruchu, temperatury, dymu, inne) zrealizowany w oparciu o minikomputer Raspberry PI 4 i modem Simcom. Element ten odpowiada za nadzorowanie bezpieczeństwa fizycznego modelowej stacji elektroenergetycznej. Multisensor wykorzystuje mechanizm MQTT (ang. *MQ Telemetry Transport*) do publikowania danych pomiarowych. Klient MQTT je subskrybuje i wyświetla (oprogramowanie Domoticz https://www.domotocz.com). Całością zarządza broker komunikatów Eclipse Mosquitto (https://mosquitto.org) zainstalowany na komputerze Serwer MQTT. Elementy Systemu 5gSTAR realizujące warstwę detekcji w układzie badawczym to system detekcji intruzów (ang. IDS, *Intrusion Detection System*) SNORT z dodatkowymi regułami dla IEC 104, system pułapkowy (ang. *Honeypot*) Conpot udający sterownik obsługujący protokół IEC 104 oraz detektor anomalii SCADA i detektor anomalii MQTT.

Ponadto, na stacji bazowej działa detektor zagłuszania i rozproszonych ataków typu odmowa usługi.

5 SPECYFIKACJA

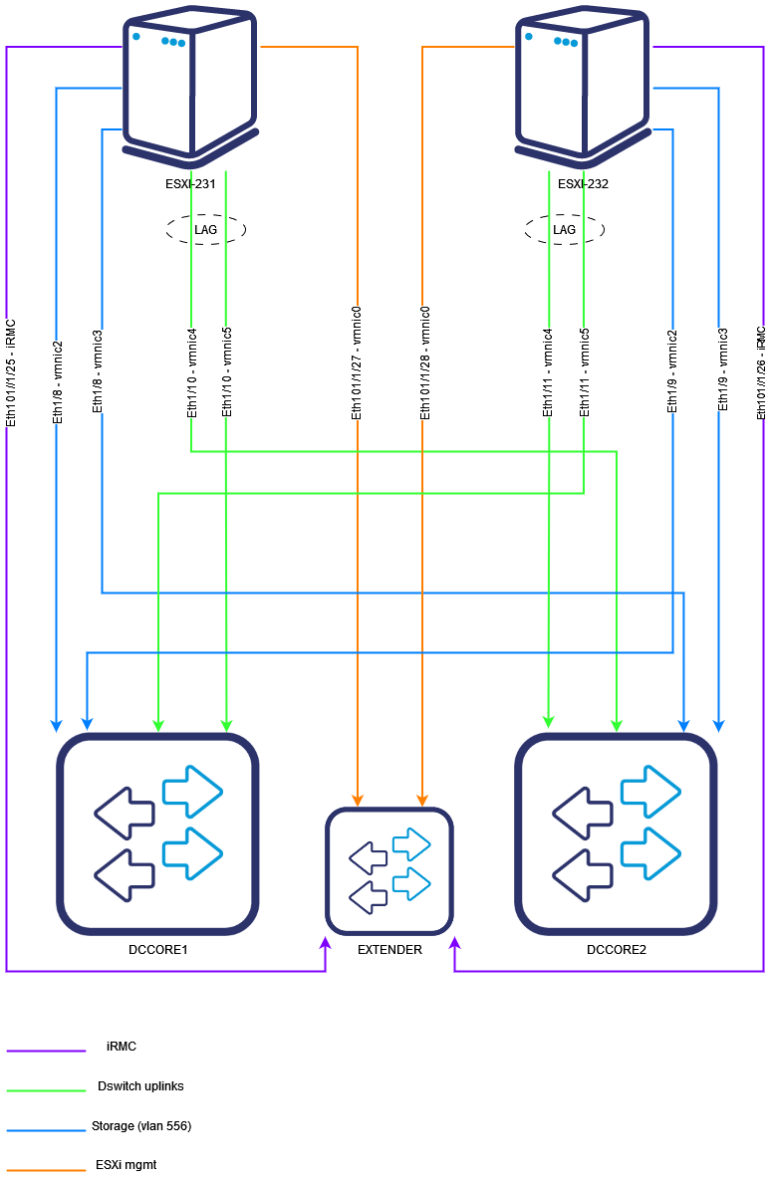
5.1 SYSTEM MONITOROWANIA

5.1.1 INFRASTRUKTURA SPRZĘTOWA

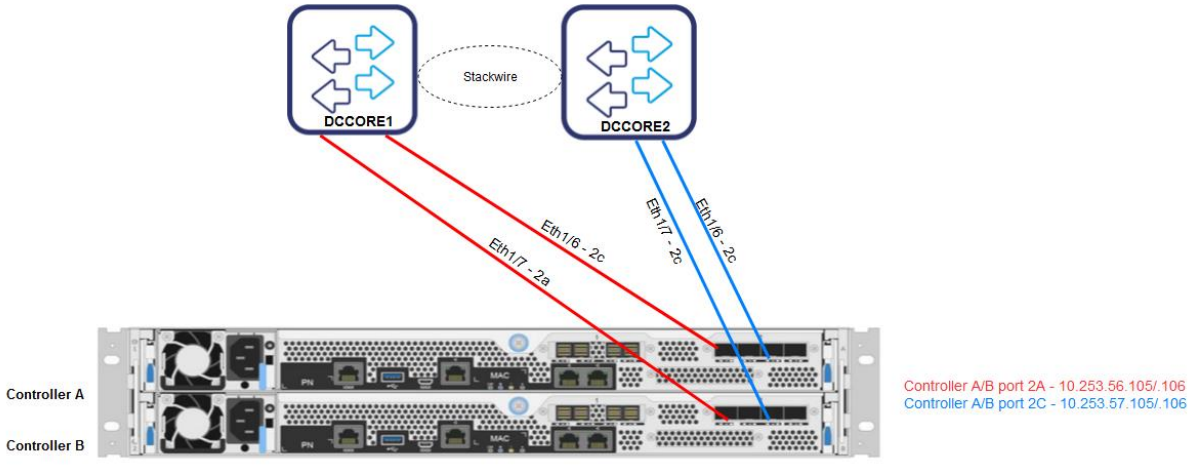
- Serwery Fujitsu PRIMERGY RX2530 M5 (2 sztuki) zapewniające wysoką wydajności i niezawodności (dedykowane do centrów danych). Wyposażone w procesory Intel Xeon Scalable, które zapewniają dużą moc obliczeniową oraz możliwość obsługi dużej liczby wirtualnych maszyn.

- Macierz dyskowa NetApp EF300 dla zastosowań wymagających wysokiej wydajności i niskich opóźnień, takich jak bazy danych, serwery plików, analiza danych i aplikacje wirtualizacyjne. Macierz wykorzystuje technologię flash, co zapewnia bardzo wysoką prędkość dostępu do danych.

Urządzenia zainstalowane zostały w serwerowni Grandmetric znajdującej się w Poznaniu. Sprzęt wykonany jest w standardzie rack, co umożliwia montaż w dedykowanych do tego szafach technicznych. Serwerownia wyposażona jest w dwa źródła zasilania, a każde z urządzeń posiada dwa zasilacze, dzięki czemu zapewniona została redundancja źródeł zasilania. W serwerowni pracuje również klimatyzacja. Urządzenia są podpięte do przełącznika Ethernet Cisco z serii Nexus (należące do Grandmetric). Wykorzystano kable światłowodowe o przepustowości 10Gb/s. Dla separacji wykorzystano segmentację VLAN oraz dedykowane podsieci IP. Opis połączeń fizycznych dla serwerów ilustruje Rysunek 13 , na którym zaznaczono redundancje połączeń zarówno dla ruchu danych do macierzy dyskowej, jak i dla ruchu zapewniającego dostęp do sieci dla maszyn wirtualnych. Z kolei Rysunek 14 prezentuje sposób połączenia do macierzy NetApp. Wykorzystane są aż 4 przewody, w celu zapewnienia bezpieczeństwa i poprawy wydajności ang. *multipathing*.



Rysunek 13 Opis połączeń pomiędzy serwerami a przełącznikiem



Rysunek 14 Opis połączeń dla macierzy NetApp

Tunel IPsec ma zapewniać bezpieczną komunikację z systemami pracującymi w infrastrukturze WIŁ-PIB. Tunel ten jest zestawiony pomiędzy urządzeniami brzegowymi typu Next-Generation Firewall obu organizacji.

Serwery Fujitsu mają zainstalowane oprogramowanie VMware ESXi i połączono je w klaster. Dzięki temu możliwe jest zarządzanie wirtualnymi maszynami (VM) poprzez jedną centralną konsolę i uzyskanie wyższej dostępności usług. W przypadku awarii jednego z serwerów, wirtualne maszyny przenoszone są automatycznie na drugi, co minimalizuje przerwy w dostępności usług. Każdy z serwerów posiada wiele interfejsów sieciowych, w tym te dedykowane do połączenia z macierzą dyskową, które obsługują protokół iSCSI (Internet Small Computer System Interface). Protokół iSCSI pozwala na podłączenie dysków twardych poprzez sieć TCP/IP do przesyłania danych pomiędzy serwerami, a macierzą dyskową. Takie rozwiązanie pozwala na uzyskanie wyższej wydajności niż w przypadku tradycyjnego połączenia z macierzą poprzez klasyczne interfejsy SAS (ang. Serial Attached SCSI) lub SATA (Serial Advanced Technology Attachment), ponieważ pozwala na wykorzystanie większej liczby interfejsów sieciowych i ich agregację.

5.1.2 ELASTIC STACK

Klaster Elasticsearch to zbiór węzłów, które współpracują ze sobą w celu przechowywania i przetwarzania danych. Węzły Elasticsearch możemy podzielić ze względu na pełnione role:

Węzeł master - jest to węzeł, który jest odpowiedzialny za zarządzanie klastrami Elasticsearch. Jest to węzeł, który podejmuje decyzje dotyczące alokacji oraz zarządzania konfiguracją klastra.

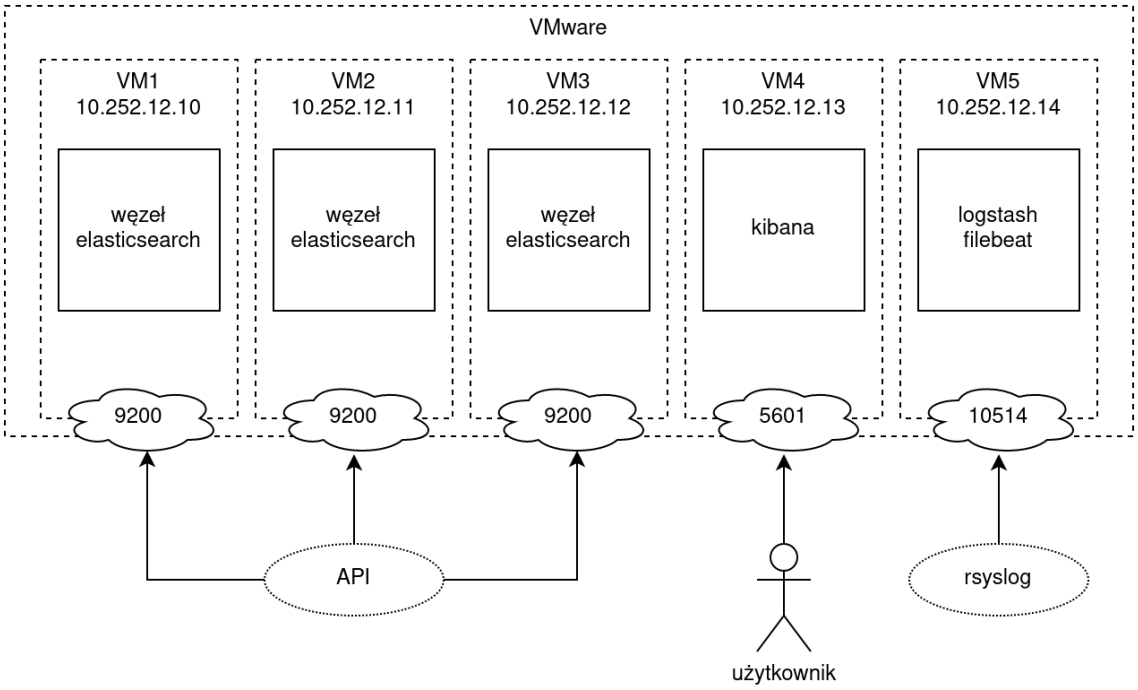
Węzeł danych- jest to węzeł, który przechowuje dane i odpowiada za ich wyszukiwanie oraz indeksowanie. Węzły danych przechowują odłamki, czyli tzw. *shardy*, które zawierają części indeksów Elasticsearch. Mogą one również pełnić rolę węzłów pośredniczących, czyli węzłów, które otrzymują żądania od klientów i przekazują je do odpowiednich węzłów danych.

Węzeł koordynujący - jest to węzeł, który odpowiada za koordynację operacji wyszukiwania i agregacji. Węzły koordynujące nie przechowują danych, ale przekazują żądania do odpowiednich węzłów danych i łączą wyniki zwrócone przez te węzły.

Węzeł ingest - jest to węzeł, który odpowiada za przetwarzanie danych przed dodaniem ich do klastra Elasticsearch. Węzły te wykonują różnego rodzaju operacje, takie jak przetwarzanie, filtracja i przekształcanie danych.

Węzeł klienta - jest to węzeł, który służy jako interfejs dla aplikacji klienta. Węzły klienta otrzymują żądania od klientów i przekazują je do odpowiednich węzłów koordynujących. Węzły klienta są często używane w celu zapewnienia wysokiej dostępności klastra Elasticsearch.

Wdrożony na potrzeby Systemu 5gSTAR przez Grandmetric klaster Elasticsearch składa się z trzech węzłów, które pełnią rolę master i data. Taki klaster zapewnia wysoką dostępność i niezawodność, a jednocześnie umożliwia skalowanie i rozproszenie danych. W tym klastrze każdy z trzech węzłów pełni obie główne role. Oznacza to, że każdy węzeł ma kopię danych i może przetwarzać zapytania związane z utrzymywanymi indeksami. Węzły będą komunikować się ze sobą w celu synchronizacji danych i koordynacji działań. W klastrze Elasticsearch każdy węzeł ma dostęp do dysku, na których będą przechowywane dane. Węzły wykorzystują mechanizm replikacji, aby zapewnić redundancje danych i minimalizować ryzyko ich utraty w przypadku awarii węzła. Interfejs użytkownika (Kibana), jest uruchomiona na osobnej maszynie wirtualnej. Źródłem danych do Elasticsearch są Logstash oraz Beats (filebeat) uruchomione na osobnej maszynie wirtualnej. Schemat opracowanego klastra Elastic Stack przedstawiono na Rysunek 15.



Rysunek 15 Schemat klastra Elastic Stack

Dostęp do Kibany, za pomocą, której można przeglądać i wizualizować dane możliwy jest na porcie 5601. Elasticsearch udostępnia na porcie 9200 API, za pomocą którego możemy wysyłać dane bezpośrednio do klastra Logstash umożliwia wysyłanie logów w formacie syslog przez port 10514. Klaster elasticsearch posiada 878GB przestrzeni do przechowywania logów i metryk, ale może z łatwością być przeskalowany w celu powiększenia dostępnej przestrzeni dyskowej. Klaster ma do dyspozycji 48GB RAM, co zapewnia płynną pracę nawet na dużej liczbie logów i metryk.

Zaproponowany w Projekcie format zdarzeń o zagrożeniach (notacja *JavaScript Object Notation, JSON*) obejmuje podstawowe dane takie jak nazwę indeksu, unikalny identyfikator, znacznik czasowy, źródło zgłaszające zdarzenie (detektor), źródło ataku, cel ataku, priorytet, komunikat informujący o szczegółach zdarzenia i wskaźnik do techniki ataku na bazie modeli MITRE. Przykład zdarzenia 5gSTAR zgłaszanego przez detektor pułapkowy Systemu 5gSTAR do Elasticsearch przedstawiono poniżej.

```
{
  "_index": "5gstar_wil_scada_honeypot",
  "_id": "rRMZQNy8tXcCAkJjGQJ1NJNf8OA",
  "_version": 1,
  "_score": 0,
  "_source": {
    "FACILITY": "user",
    "destination": {"port": "2404", "ip": "127.0.1.1"},
    "HOST": "conpot-VirtualBox",
    "PRIORITY": "notice",
    "source": {"port": "42298", "ip": "12.0.0.1"},
    "network": {"transport": "TCP"},
    "ISODATE": "2024-02-05T11:59:20.469123+00:00",
    "@timestamp": "2024-02-05T11:59:20.469153+00:00",
    "MESSAGE": "New IEC 104 connection from 12.0.0.1:42298.\n('12.0.0.1', 42298) ---
> s_frame receive nr: 0.",
    "threat": {"technique": {"id": "T0832"}},
    "event": {"severity": "4"},
    "PROGRAM": "conpot"
  },
  "fields": {
    "MESSAGE.keyword": ["New IEC 104 connection from 12.0.0.1:42298.\n('12.0.0.1', 42298) -
--> s_frame receive nr: 0."],
    "destination.port": ["2404"],
    "HOST": ["conpot-VirtualBox"],
    "PRIORITY": ["notice"],
    "MESSAGE": ["New IEC 104 connection from 12.0.0.1:42298.\n('12.0.0.1', 42298) ---
> s_frame receive nr: 0."],
    "ISODATE": ["2024-02-05T11:59:20.469Z"],
    "source.ip": ["12.0.0.1"],
    "FACILITY.keyword": ["user"],
    "HOST.keyword": ["conpot-VirtualBox"],
    "event.severity": ["4"],
    "source.port.keyword": ["42298"],
    "destination.port.keyword": ["2404"],
    "FACILITY": ["user"],
    "event.severity.keyword": ["4"],
    "PROGRAM.keyword": ["conpot"],
    "PRIORITY.keyword": ["notice"],
    "threat.technique.id": ["T0832"],
    "network.transport.keyword": ["TCP"],
    "destination.ip": ["127.0.1.1"],
    "network.transport": ["TCP"],
    "threat.technique.id.keyword": ["T0832"],
    "destination.ip.keyword": ["127.0.1.1"],
    "@timestamp": ["2024-02-05T11:59:20.469Z"],
    "source.port": ["42298"],
    "source.ip.keyword": ["12.0.0.1"],
    "PROGRAM": ["conpot"]
  }
}
```


Dzięki specyfikacji ECS (Elastic Common Schema - https://www.elastic.co/guide/en/ecs/current/ecs-reference.html) możliwe jest łatwe zestawienie na wspólnych widokach danych pochodzących z różnych źródeł. ECS opisuje w jaki sposób powinny być sformatowane dane, aby były one zgodne np. z modułami stosu Elastic takimi jak auditbeat czy filebeat. ECS nie jest narzędziem, które dokonuje normalizacji, a jedynie zestawem dobrych praktyk. ECS pozwala rozwiać wątpliwości dotyczące np. nazwy pola w strukturze, w którym chcemy przesłać hostname danego urządzenia.

Posiadając znormalizowane dane możemy je łatwo filtrować, agregować i wizualizować.

Dane przekazywane do elasticsearch przez narzędzia wykrywające zagrożenia powinny w miarę możliwości ich konfiguracji raportować dane zgodnie ze specyfikacją ECS. Nie jest to jednak twardym wymaganiem, gdyż baza elasticsearch pozwala na zdefiniowanie przetwarzania danych przed ich indeksowaniem. Przetwarzanie to realizowane jest na poziomie indeksu, a biorąc pod uwagę, że różne narzędzia mogą wymagać różnego przetwarzania zaleca się, aby każde narzędzie raportowało dane do osobnego indeksu w elasticsearch zgodnie ze schematem nazewnictwa:

5gstar_{organizacja}_{obszar}_{narzędzie}

np. 5gstar_wil_scada_snort3

W ten sposób, jeśli narzędzie snort3 będzie wysyłało dane dotyczące hostname w polu o nazwie „HOSTNAME" w procesie przetwarzającym dla tego indeksu można zdefiniować krok *rename*, który zmieni nazwę tego pola na zgodne z ECS, czyli „host.hostname".

5.1.3 PROJEKT APLIKACJI MONITOROWANIA I REAGOWANIA

Głównym zadaniem opartej o narzędzie Kibana Aplikacji Monitorowania ma być wizualizacja danych zebranych w bazie elasticsearch. Pulpit Aplikacji Monitorowania powinien być punktem początkowym pracy specjalisty ds. bezpieczeństwa. Na pulpicie powinna być widoczna liczba zagrożeń, najczęściej występujące typy zagrożeń, umiejscowienie zagrożeń na osi czasu oraz możliwość przejścia z danego zagrożenia do aplikacji umożliwiającej mitygację (Aplikacja do Mitygacji Zagrożeń).

Ze względu na ograniczenia Kibany, która z założenia jest narzędziem do wizualizacji i poza filtrowaniem danych nie umożliwia stworzenia pulpitu, w którym mogłyby być podejmowane akcje konieczne jest stworzenie dodatkowego składnika, który dla danego zagrożenia wyświetli podsumowanie, rekomendowane mitygacje wskazywane przez bazę MITRE oraz umożliwi mitygację danego zagożenia w sposób predefiniowany dla konkretnego narzędzia oraz obszaru sieci w jakiej zostało ono wykryte.

Aplikacja do mitygacji zagrożeń powinna był połączona ze stosem Elastic za pomocą:

- REST API z elasticsearch w celu pobierania i zapisywania danych

- Adresy URL w Kibanie oraz aplikacji do mitygacji umożliwiające swobodne przełączanie się pomiędzy widokami części wizualizacyjnej i mitygacyjnej

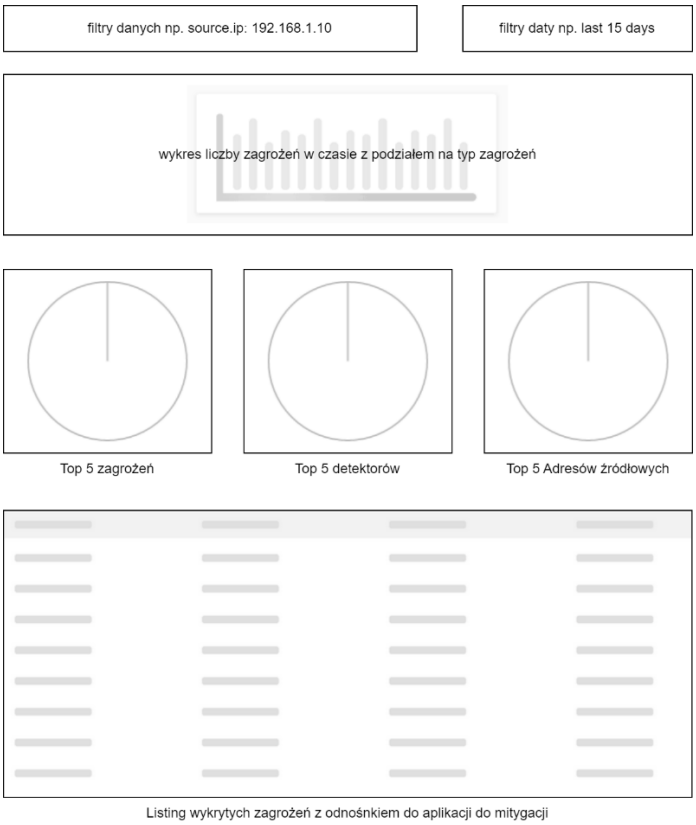
Ze względu na konieczność komunikacji z wykorzystaniem API elasticsearch i stosunkowo niewygórowane wymagania dotyczące części wizualizacyjnej aplikacji do mitygacji preferowaną metodą implementacji jest jeden z frameworków w języku Python umożliwiający tworzenie aplikacji web np. *django*, *pyvibe* czy *reactpy*.

W ramach aplikacji dostępne powinny być następujące akcje:

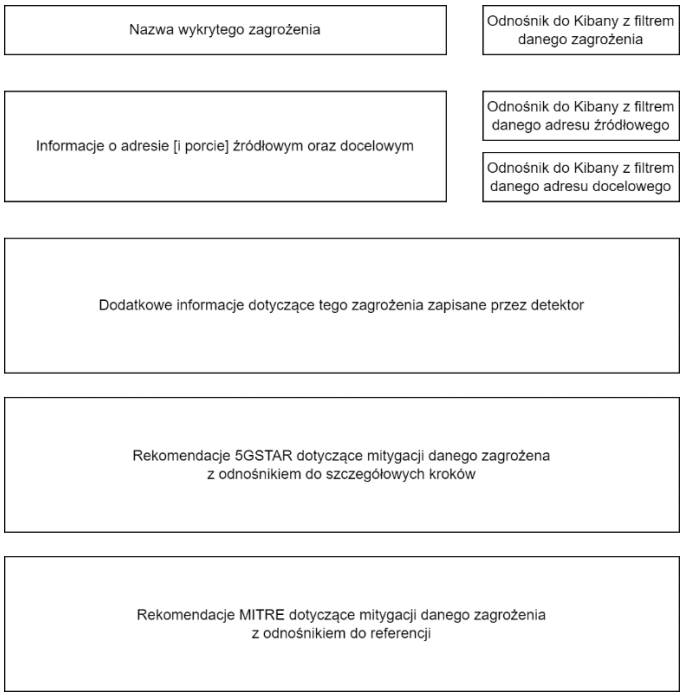
- Szczegółowy podgląd danych dotyczących danego zagrożenia przesłanych przez narzędzie, które to zagrożenie wykryło
- Rekomendacje MITRE dotyczące mitygacji danego typu zagrożenia
- Rekomendacje 5gSTAR dotyczące mitygacji danego typu zagrożenia

Możliwość raportowania wykonania danego typu zagrożenia

Poniżej przedstawione projekt UX (ang. *User Experience*) Aplikacji Monitorowania i Aplikacji do Mitygacji Zagrożeń (reagowania).



Rysunek 16 Widok główny Aplikacji Monitorowania



Rysunek 17 Widok główny Aplikacji do Mitygacji Zagrożeń

W zakresie bezpieczeństwa rozwiązania należy przyjąć założenia zaprezentowane poniżej:

Elasticsearch z autoryzacją typu *basic auth*, która wymaga podania nazwy użytkownika oraz hasła. Dodatkowo dostęp do Aplikacji Monitorowania (Kibana) ograniczony jedynie dla istniejących użytkowników, a sama aplikacja powinna umożliwiać zarządzanie istniejącymi użytkownikami (tj. dodawanie, usuwanie i edytowanie). Aplikacja powinna wykorzystywać certyfikat SSL i być dostępna na porcie 443 wykorzystując protokół HTTPS. Dopuszcza się, że wykorzystywany certyfikat będzie certyfikatem typu *self-signed*, który w przyszłości może zostać podmieniony na certyfikat uznany za zaufany przez urząd certyfikacji. Dostęp do aplikacji do mitygacji powinien również być zabezpieczony i może wykorzystywać autoryzacje z wykorzystaniem tokenu przekazanego w nagłówku zapytania lub bezpośrednio jako jeden z parametrów zapytania (query).

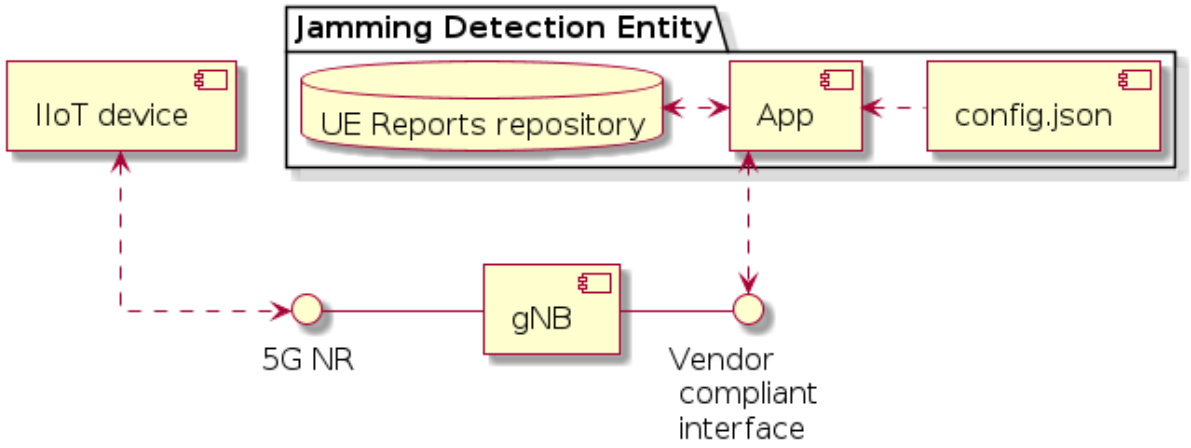
5.2 AUTORSKIE DETEKTORY I ELEMENTY REAKCJI

5.2.1 DETEKTOR ZAGŁUSZANIA W RAN

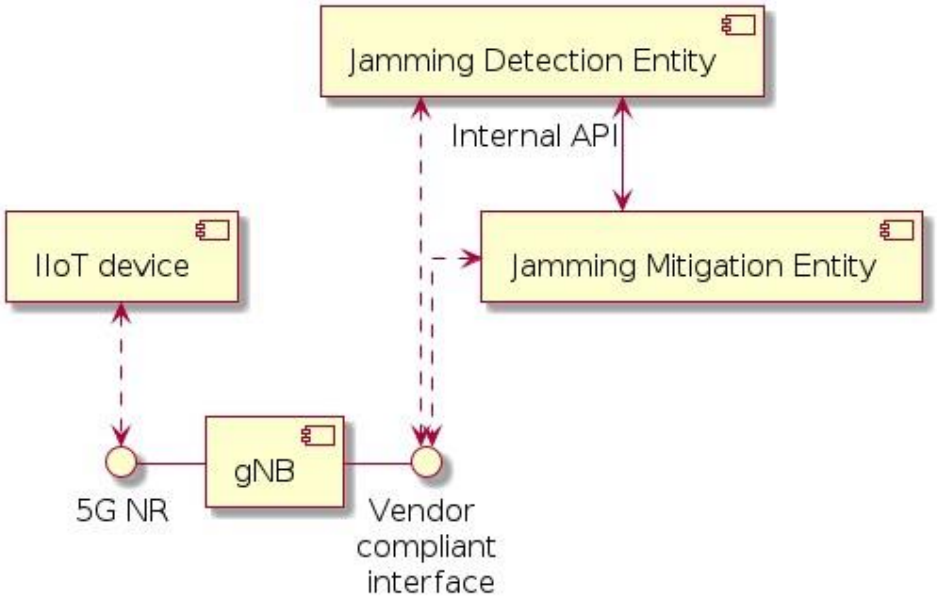
W ramach prac badawczych prowadzonych w Projekcie zaproponowano metodę detekcji i łagodzenia efektów ataku polegającego na zagłuszaniu (ang. *jamming*) stacji bazowych 5G (gNB) [4][5]. Atak i jego detekcja oraz łagodzenie ma miejsce w na sieci dostępowej RAN

(ang. *Radio Access Network*). Algorytm wykorzystuje uczenie nienadzorowane KNN (K-najbliższych sąsiadów). Detekcja polega na monitorowaniu jakości łącza radiowego, a mitygacja na zmianie schematu modulacji i kodowania.

Na Rysunek 18 i Rysunek 19 przedstawiono projekt w postaci diagramów UML komponentów dla opracowanej metody. Schemat obejmuje urządzenia Internetu Rzeczy IIoT (ang. *Industrial Internet of Things*), stacje bazowe 5G (gNB), Jednostki Wykrywania Ataków i Jednostki Łagodzenia Ataków. Jednostka Łagodzenia Ataków komunikuje się poprzez wewnętrznie zdefiniowany protokół (np. HTTP, modyfikację wpisów w bazie danych lub plików konfiguracyjnych) z Jednostką Wykrywania Ataków, która wysyła informację o wykryciu ataku typu *jamming*. Jednostka Łagodzenia Ataków, podobnie jak Jednostka Wykrywania Ataków komunikuje się ze stacją bazową za pomocą interfejsu zdefiniowanego przez dostawcę sprzętu gNB, który umożliwia monitorowanie raportów jakości poszczególnych łączy i zmianę konfiguracji.

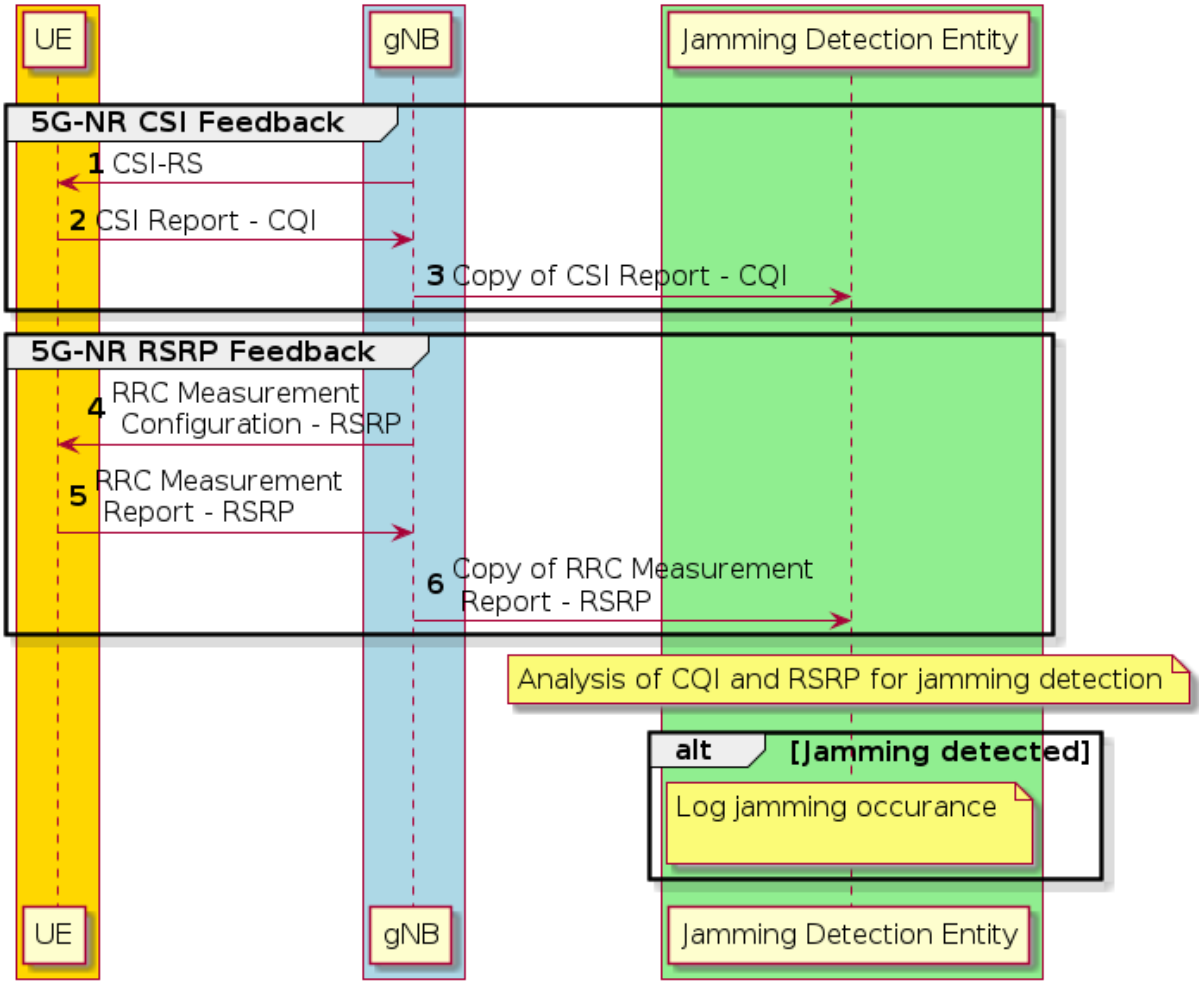


Rysunek 18 Diagram UML komponentów dla mechanizmu wykrywania ataków typu jamming

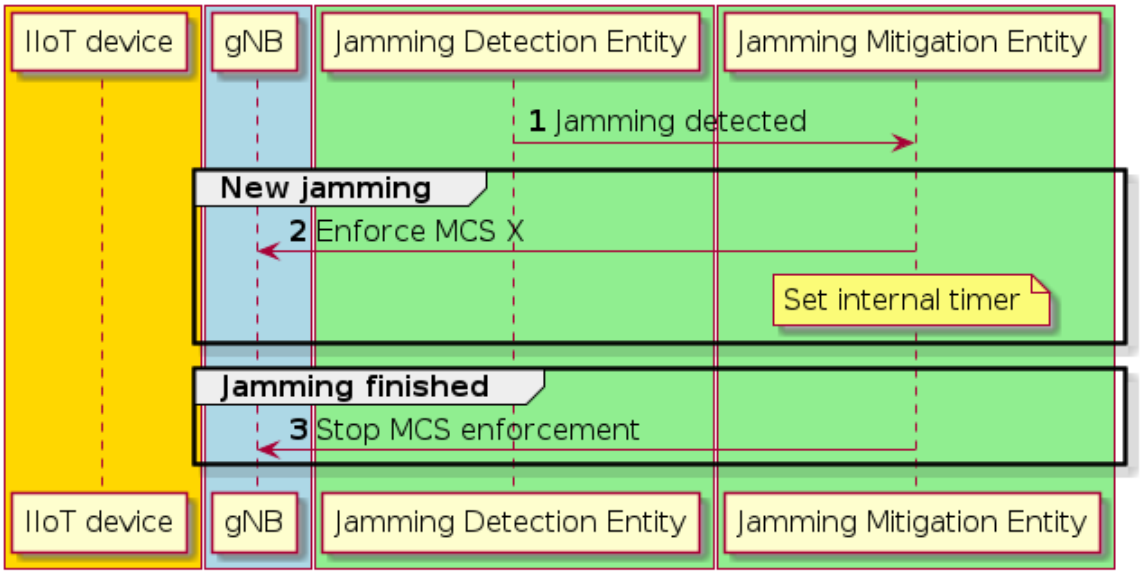


Rysunek 19 Diagram UML komponentów dla mechanizmu łagodzenia ataków typu jamming

Diagramy UML sekwencji związane z metodą wykrywania i łagodzenia *jammingu* przedstawiono na Rysunek 20 i Rysunek 21. Zaprezentowano tu wymianę wiadomości przy wykryciu zagłuszania i jego łagodzenia (w następstwie wykrycia). Informacja o wykryciu jest przesyłana z Jednostki Wykrywania Ataków do Jednostki Łagodzenia Ataków celem odpowiedniego wysterowania stacji bazowej.



Rysunek 20 Diagram UML sekwencji dla mechanizmu detekcji ataków typu jamming

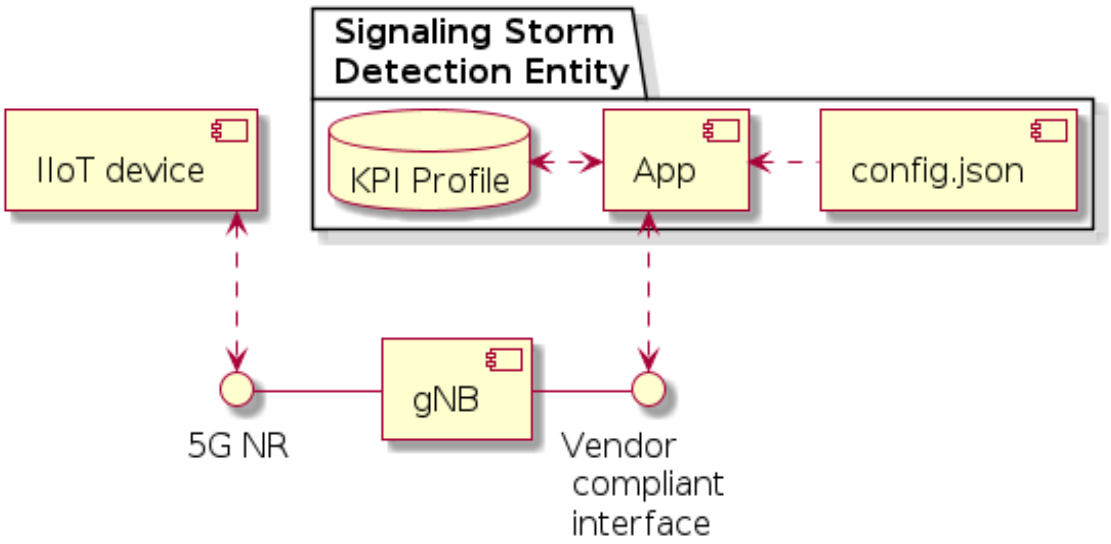


Rysunek 21 Diagram UML sekwencji dla mechanizmu łagodzenia ataków typu jamming

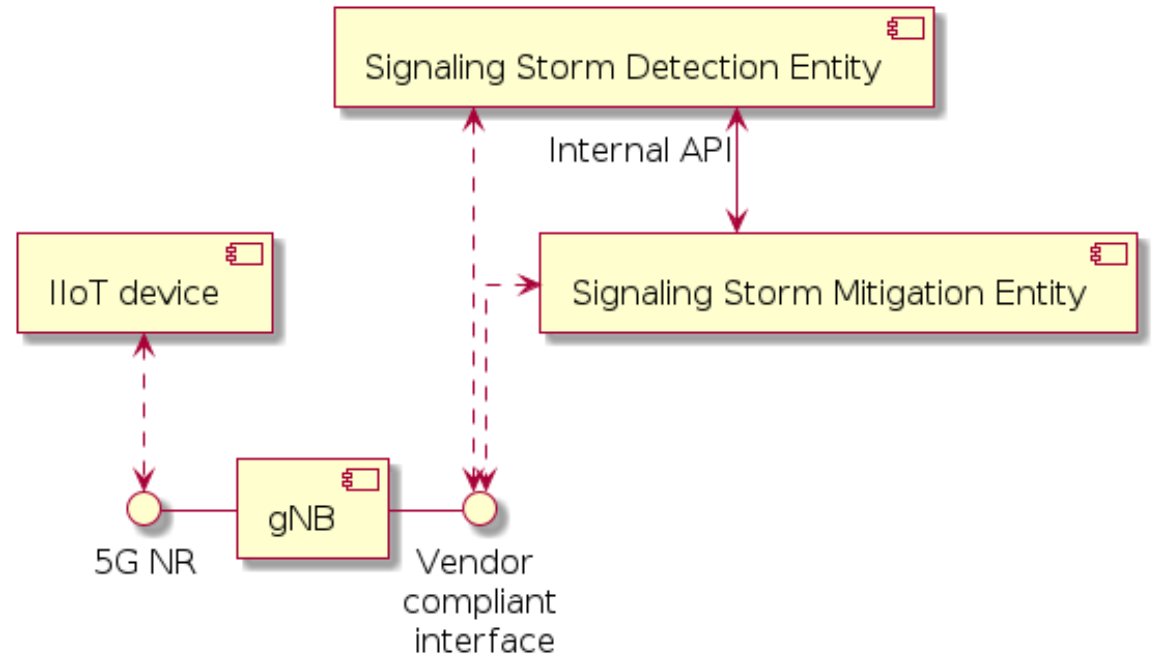
5.2.2 DETEKTOR ATAKU TYPU ROZPROSZONA ODMOWA USŁUGI W RAN

Kolejną metodą opracowana w Projekcie jest detekcja i łagodzenie ataków typu *signaling storm /Distributed Denial of Service* na sieć dostępową RAN [4][5]. Metoda opiera się na wykorzystaniu tzw. Profili KPI (ang. *Key Preformance Indicator Profile*), które przechowują w tym przypadku średnią i odchylenie standardowe liczby zgłoszeń terminali 5G np. urządzeń przemysłowego Internetu Rzeczy do sieci przypadającą na zadany przedział czasowy. Na podstawie Profilu KPI oraz aktualnie zaobserwowanej liczbie zgłoszeń do sieci 5G obliczane są tzw. wartości anomalii, będące danymi wejściowymi do ważonej wersji algorytmu grupującego DBSCAN, którego rezultatem jest decyzja o wykryciu (lub niewykryciu) ataku typu *signaling storm*.

Na Rysunek 22 i Rysunek 23 przedstawiono projekt rozwiązania w postaci diagramów UML komponentów. Składa się ono w ogólności z 4 komponentów: Urządzenia IIoT, stacji bazowej 5G – gNB, Jednostki Wykrywania Ataków i Jednostki Łagodzenia Ataków.

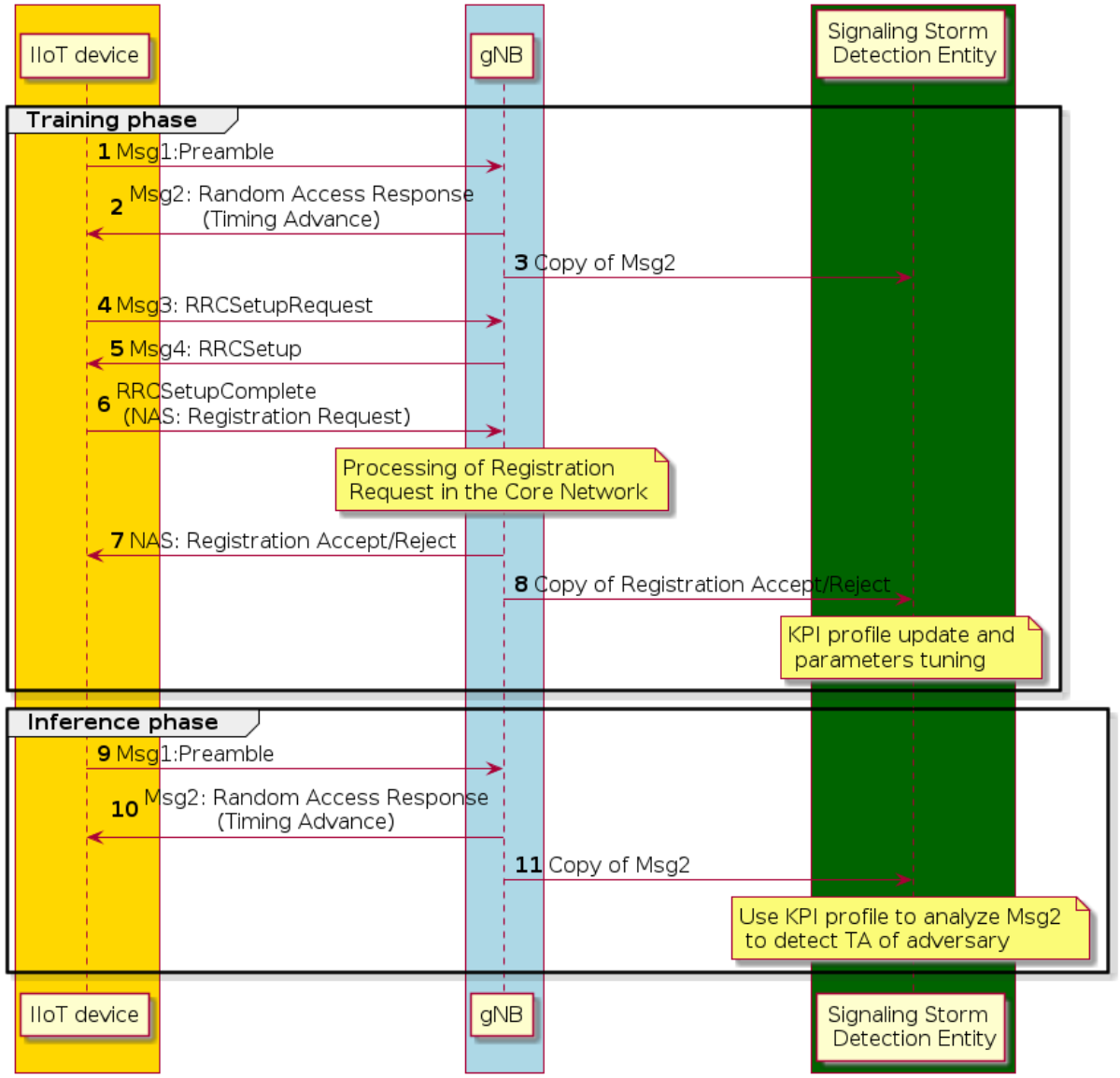


Rysunek 22 Diagram UML komponentów dla mechanizmu wykrywania ataków typu signaling storm

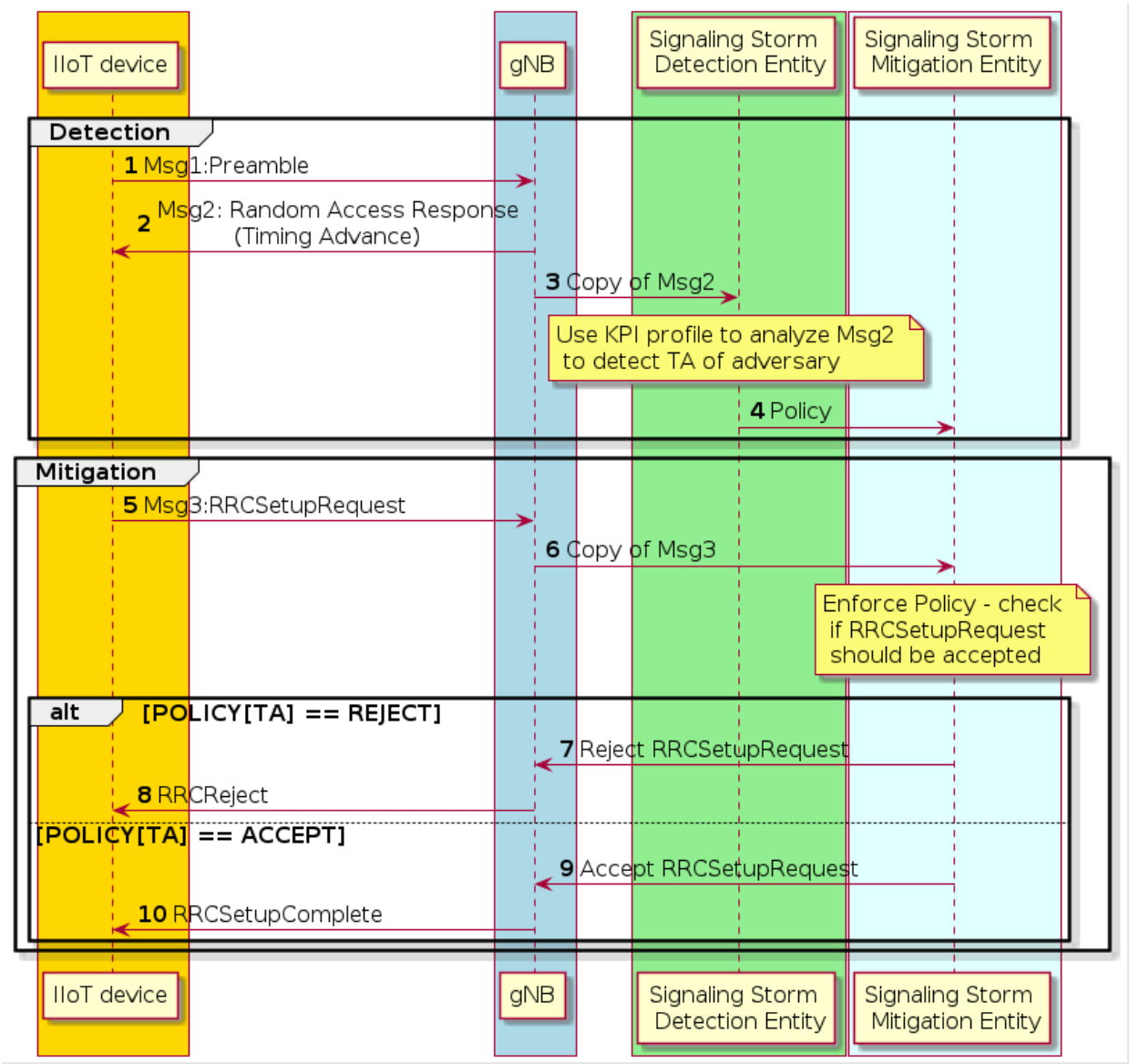


Rysunek 23 Diagram UML komponentów dla mechanizmu przeciwdziałania atakom typu signaling storm

Diagramy UML sekwencji związany z metoda wykrywania i łagodzenia ataków typu *signaling storm* są przedstawione na Rysunek 24 i Rysunek 25.



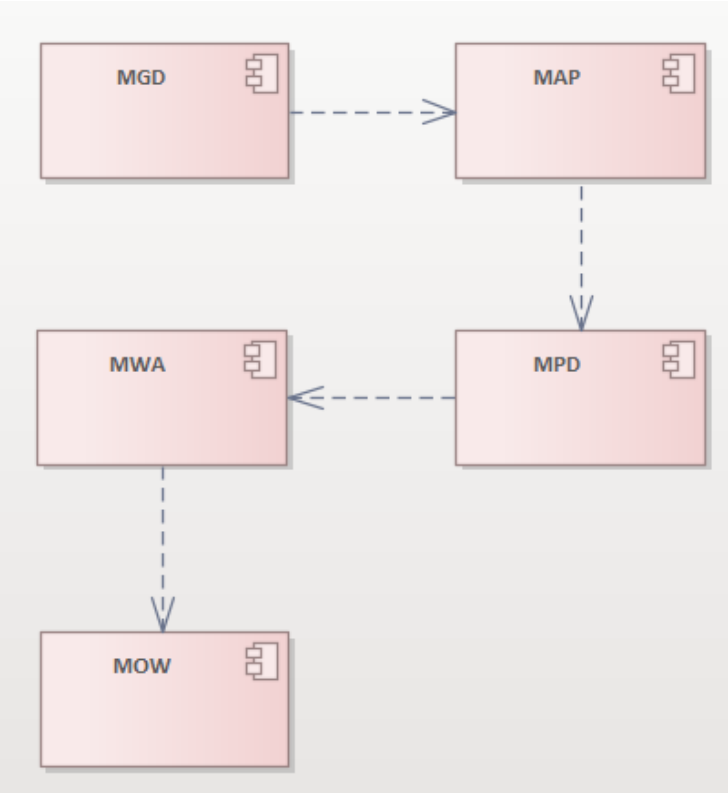
Rysunek 24 Diagram UML sekwencji dla mechanizmu wykrywania ataków typu signaling storm



Rysunek 25 Diagram UML sekwencji dla mechanizmu przeciwdziałania atakom typu signaling storm

5.2.3 Detektor Anomalii SCADA i IIoT

W ramach innych prac badawczych opracowano detektory anomalii w ruchu sieciowym SCADA (protokoły IEC) i IIoT (protokół MQTT) bazujące na uczeniu maszynowym (m.in. algorytm OneClassSVM) [2][3]. Projekt w postaci diagramu komponentów dla w/w rozwiązania przedstawiono na Rysunek 26.

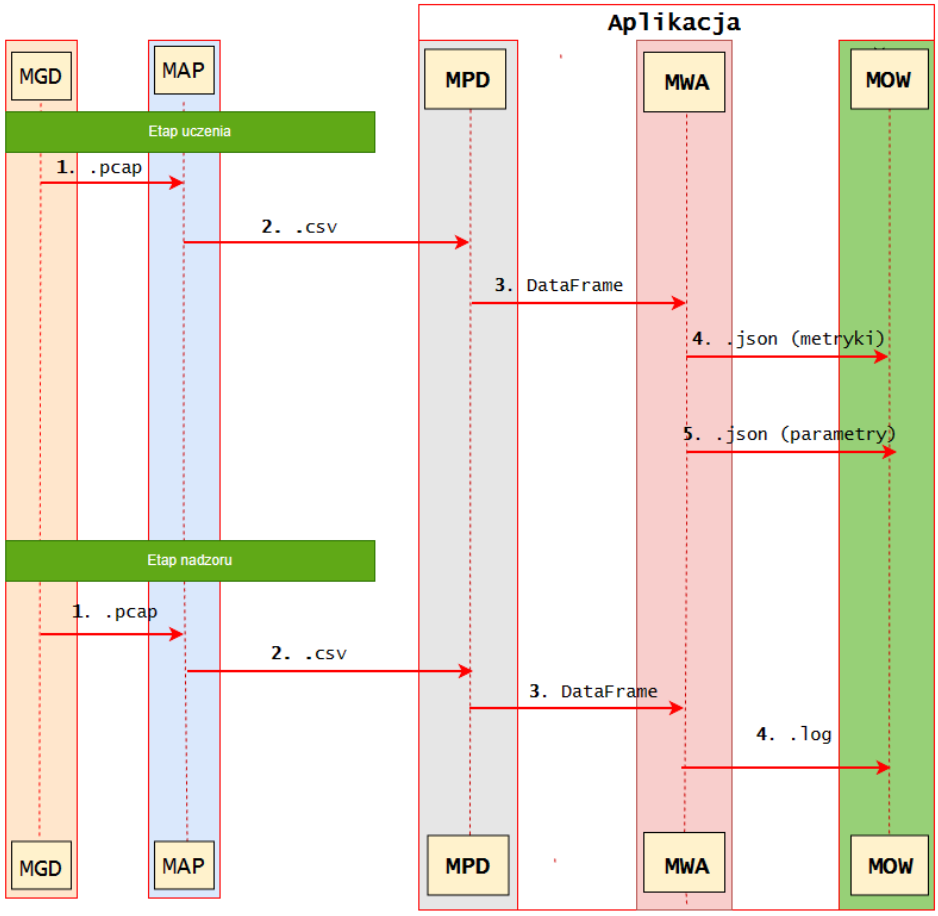


Rysunek 26 Diagram UML komponentów dla mechanizmu wykrywania anomalii w sieci SCADA i IIoT

Detektor jest zbudowany z kilku współpracujących modułów, które są odpowiedzialne za różne etapy procesu wykrywania anomalii w przepływach sieciowych. Pierwszym modułem jest MGD (Moduł Gromadzenia Danych), który wykorzystuje narzędzie tshark do przechwytywania pakietów w sieci. MGD zbiera dane z ruchu sieciowego w czasie rzeczywistym, umożliwiając dalszą analizę. Kolejnym modułem jest MAP (Moduł Analizy Przepływów), który opiera się na narzędziu CICFlowMeter. MAP analizuje zgromadzone dane pakietów i generuje przepływy, czyli logiczne grupy pakietów opisujące interakcje między różnymi źródłami i docelowymi adresami. Przepływy zawierają kluczowe informacje na temat ruchu sieciowego pod kątem wykrywania anomalii. Następnie, dane z przepływów są przekazywane do MPD (Moduł Przetwarzania Danych), gdzie realizowana jest ekstrakcja cech i standaryzacja. MPD wyciąga istotne atrybuty/cechy z przepływów, które stanowią podstawę dla dalszego etapu wykrywania anomalii. Ponadto, cechy są standaryzowane, aby utrzymać spójność i ułatwić przetwarzanie przez algorytmy. Najbardziej złożonym modułem systemu jest MWA (Moduł Wykrywania Anomalii), który wykorzystuje algorytm uczenia maszynowego, np. OneClassSVM. MWA analizuje znormalizowane cechy przepływów i identyfikuje potencjalne anomalie w ruchu sieciowym. Model np. OCSVM uczy się reprezentatywnych wzorców ruchu sieciowego, co pozwala na efektywne wykrywanie odstających zachowań. Ostatnim modułem jest MOW (Moduł Oceny Wyników), który pełni

rolę zarówno na etapie uczenia, jak i pracy. Na etapie uczenia, MOW ocenia wydajność modelu za pomocą różnych metryk oceny, takich jak dokładność, precyzja, czułość itp. W trakcie nadzoru systemu, MOW wnioskuje na podstawie wyników wykrywania anomalii, generuje raporty, powiadamia użytkowników o potencjalnych zagrożeniach i podejmuje odpowiednie działania. Wszystkie moduły współpracują ze sobą, przetwarzając dane w sposób sekwencyjny i iteracyjny, aby umożliwić skuteczne wykrywanie anomalii w ruchu sieciowym. Architektura rozwiązania została zaprojektowana tak, aby zautomatyzować proces analizy ruchu sieciowego i zapewnić efektywny monitoring i wykrywanie nieprawidłowości w sieci.

Diagram sekwencji dla mechanizmu wykrywania anomalii w sieci SCADA i IIoT zaprezentowano na Rysunek 27.



Rysunek 27 Diagram sekwencji dla mechanizmu wykrywania anomalii w sieci SCADA i IIoT

Sekwencja działania na etapie uczenia:

MGD (Moduł Gromadzenia Danych) używa narzędzia tshark do przechwycenia pakietów z pliku .pcap. Dane pakietów przekazywane są do MAP (Moduł Analizy Przepływów), który wykorzystuje narzędzie CICFlowMeter do przetwarzania pakietów na przepływy i zapisuje je w formacie .csv. Moduł MAP przekazuje przepływy w formacie .csv do MPD (Moduł Przetwarzania Danych), gdzie następuje ekstrakcja cech i utworzenie DataFrame'a. DataFrame z znormalizowanymi cechami przepływów przekazywany jest do MWA (Moduł Wykrywania Anomalii), gdzie jest używany algorytm uczenia maszynowego np. One-Class SVM do nauczenia modelu i znalezienia granicy decyzyjnej. MWA zwraca parametry modelu w formacie .json do MOW (Moduł Oceny Wyników), który służy do oceny wydajności modelu na etapie uczenia i ewentualnej optymalizacji parametrów.

Sekwencja działania na etapie detekcji:

MGD (Moduł Gromadzenia Danych) używa narzędzia tshark do przechwycenia pakietów z pliku .pcap. Dane pakietów przekazywane są do MAP (Moduł Analizy Przepływów), który wykorzystuje narzędzie CICFlowMeter do przetwarzania pakietów na przepływy i zapisuje je w formacie .csv. Moduł MAP przekazuje przepływy w formacie .csv do MPD (Moduł Przetwarzania Danych), gdzie następuje ekstrakcja cech i utworzenie DataFrame'a. DataFrame z znormalizowanymi cechami przepływów przekazywany jest do MWA (Moduł Wykrywania Anomalii), gdzie jest używany algorytm uczenia maszynowego np. One-Class SVM do wykrywania anomalii. MWA wysyła wykryte anomalie w formacie .log do MOW (Moduł Oceny Wyników), który posiada interfejs do oceny uzyskanych w trakcie nadzoru wyników.

6 BIBLIOGRAFIA

[1]. Wniosek o projekt Zaawansowane metody i techniki wykrywania i przeciwdziałania atakom na infrastrukturę dostępową i aplikacje sieci 5G - 5gSTAR, 2021
[2]. Zespół WIŁ-PIB I PP, P4.1. Projekt mechanizmów identyfikacji ataków na aplikacje sieci 5G, 5gSTAR, 2023
[3]. Zespół WIŁ-PIB I PP, P4.2. Raport z weryfikacji mechanizmów identyfikacji ataków na aplikacje sieci 5G, 5gSTAR, 2023
[4]. Hanna Bogucka, Marcin Hoffmann, Paweł Kryszkiewicz, Łukasz Kułacz, Implementacja wybranych metod identyfikacji i przeciwdziałania atakom na sieci dostępowe 5G, 5gSTAR, 2024
[5]. Hanna Bogucka, Marcin Hoffmann, Paweł Kryszkiewicz, Łukasz Kułacz, Przeprowadzenie badań metod identyfikacji i przeciwdziałania atakom na sieci dostępowe 5G, 5gSTAR, 2024
[6]. Przemysław Bereziński, Weryfikacja wymagań na system 5gSTAR, 5gSTAR, 2024
[7]. P. Kobziakowski, „Elastic Blog", 17 Czerwiec 2020. [Online]. Dostępny pod adresem: https://www.elastic.co/blog/telecommunications-observability-elastic-stack-monitoring-voice-traffic-data
[8]. Elastic, „Elastic Observability", 03 2023. [Online]. Dostępny pod adresem: https://www.elastic.co/customers/verizon-wireless
[9]. OpenAirInterface.org, „OPENAIRINTERFACE," [Online]. Available: https://openairinterface.org/
[10]. https://docs.srsran.com/projects/project/en/latest/dev_guide/source/software_arch/source/index.html [Online]
[11]. O-RAN Alliance, O-RAN.WG3.E2SM-RC-v01.01, "O-RAN Near-Real-time RAN Intelligent Controller E2 Service Model (E2SM), RAN Control", 2022.
[12]. Amarisoft, „Amarisoft 4G 5G from the lab to the field," [Online]. Available: https://www.amarisoft.com/
[13]. Aether, „Aether," [Online]. Available: https://aetherproject.org/
[14]. Open5gs, „Open5GS," [Online]. Available: https://open5gs.org/
[15]. 3GPP TS 23.501 Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2 (Release 17, V17.2.0), Geneva: 3GPP, 2021.
[16]. R. Zhang, Y. Lin, S. Chen i Z. Mo, „A Multi-Node 5G Core Network Testbed Developed from Open5GS," w 9th International Conference on Computer and Communications (ICCC), Chengdu, 2023.
[17]. C. Choudhari, R. Patil i S. Saraf, „Deployment of 5G Core for 5G Private Networks," w International Conference on Industry 4.0 Technology (I4Tech), Pune, 2022.