5G Core Implementation Comparison

Parsa Kootzari 101316375

May Wang 101099445

Content

- Introduction
- High Level Goal
- Performance Evaluation
- Security Evaluation
- Challenges
- Next Steps

Introduction

- The three main component of 5G are:
  - 5G Core
  - 5G Radio Access Network (RAN)
  - User Equipment (UE)
- Currently there are two main implementations of 5G Core:
  - Free5GC: Implemented in Go language
  - Open5GS: Implemented in C language

High Level Goals

- Make a comparison between the two 5G core implementations.
- Two main aspects of comparison:
  - Performance evaluation
  - Security evaluation

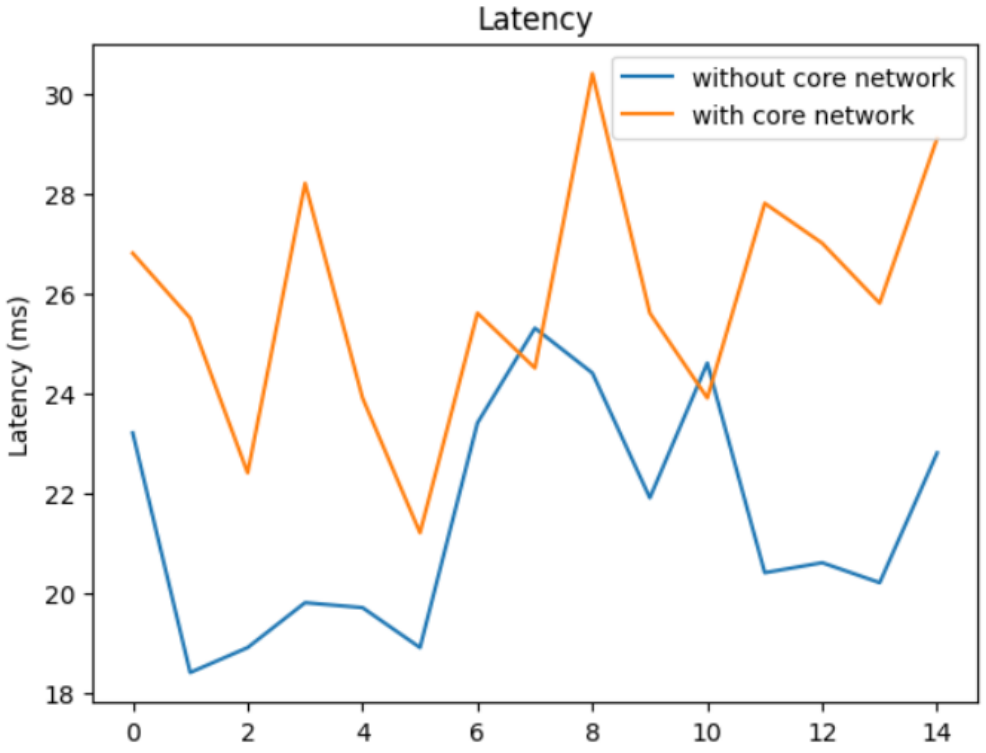
Performance Comparison Overview

- Deploy each 5G core implementation on the isolated environment with the same configurations.
- Deploy UERANSIM and connect it to the 5G core network.
- Measure the Uplink and Downlink throughput of each network.
- Measure the latency of each network.
- Make comparison between measurement from 5G core network and native network of the VM without 5G core.
- Measure the resource consumption of 5G implementation.

Environment Setup

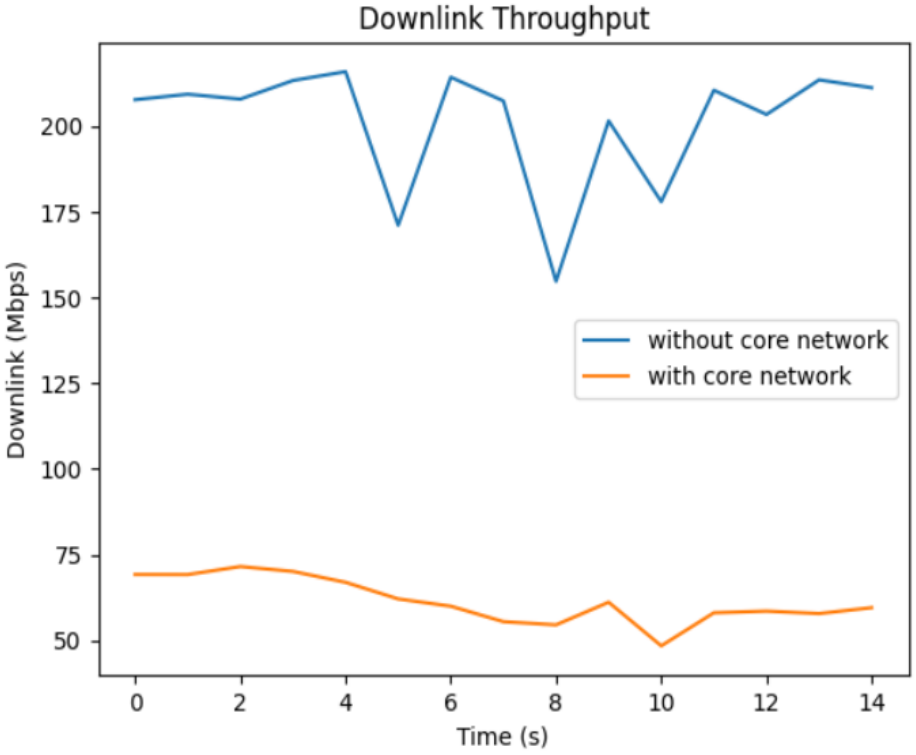
- Deployment Environment:
  - Personal Laptop with 8GB RAM and Intel i5 1135G7
- For Free5GC:
  - First VM with 2GB RAM + 2 CPU Cores for Free5GC deployment
  - Second VM with 2GB RAM + 2 CPU Cores for UERANSIM deployment.
- For Open5GS:
  - Same configurations for VMs
  - Not fully functional yet
- 5G core networks are deployed natively on the VM

Latency



- Single UE
- Using Ping command
- By changing the interface
  - -I `uesimtun0`

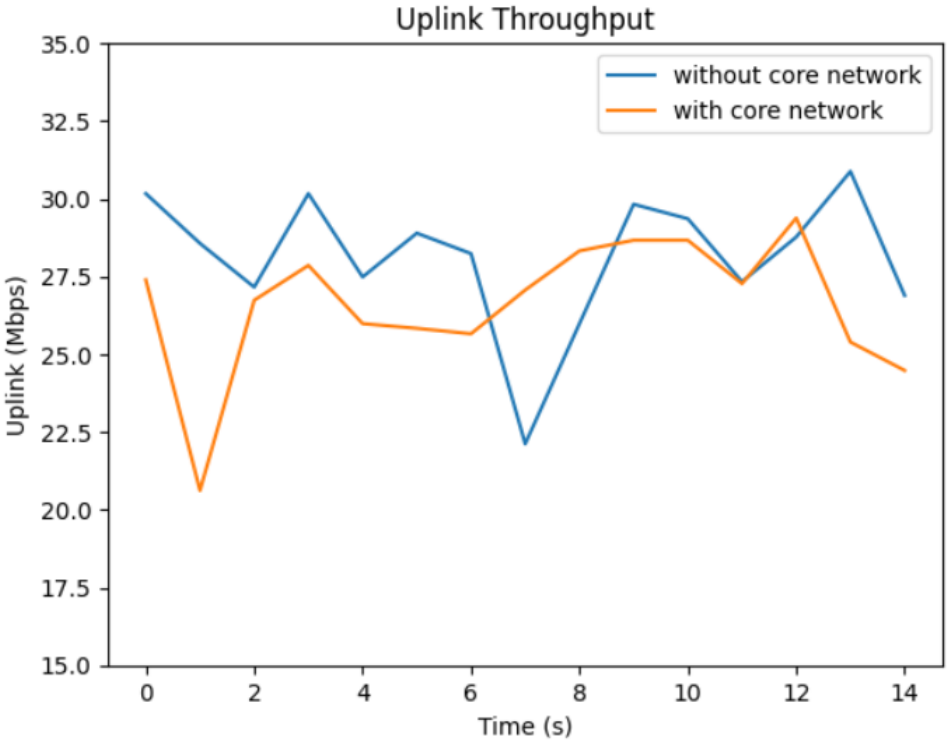
Downlink



- Speedtest CLI
- Change the default interface to `uesimtun0`
- Same result with this command:

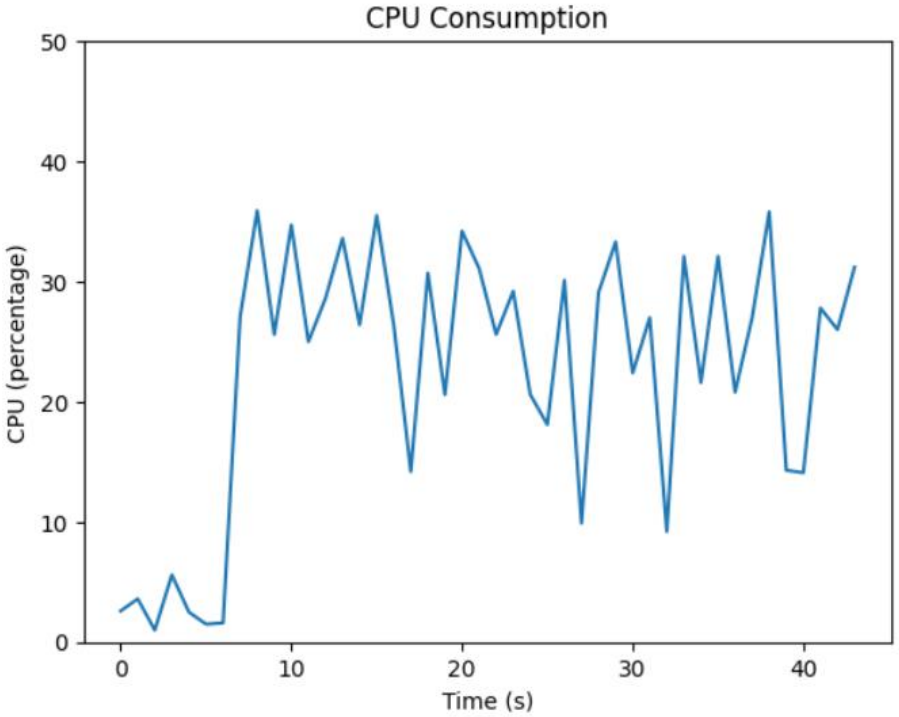
```
wget –bind-interface=<uesimtun0-IP>
```

Uplink



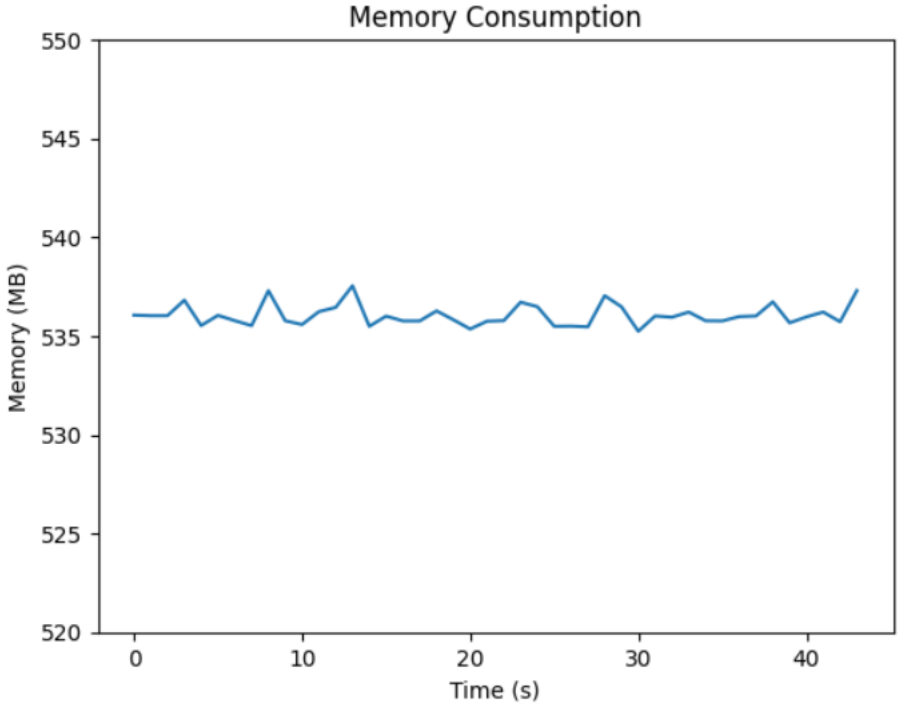
- Speedtest CLI
- Change the default interface to `uesimtun0`
- Not attributed to the UE downlink and uplink speed limit:
  - 2000Mbps downlink
  - 1000Mbps uplink

Resource Consumption



- The first part is when the UE is not sending any traffic.
- The peak is when UE is using the network.
- CPU usage Mean: 27%

Resource Consumption



- No apparent changes in the memory when UE is using the core network.
- Initial memory usage of OS is between 220 and 250 MB.
- Memory usage of Free5GC is around 300MB.

Security Scan Tools – Docker Container Image

Clair

- Container Register with a built-in security scan
- Quay: security scan result for any image
- Clair: Container Registry + Quay
  - It examines the **layers of container images and their associated packages** to detect vulnerabilities.
  - Including the National Vulnerability Database (NVD) and CoreOS's own vulnerability database.

Trivy

- It scans container images by **inspecting the filesystem and analyzing package manifests** to identify vulnerable software components.
- Uses a comprehensive vulnerability database that includes data from multiple sources such as NVD, Red Hat, Alpine, and more.

Security Metric - Common Vulnerability Scoring System (CVSS)

- CVSS is a standardized system for assessing and scoring the severity of security vulnerabilities in software systems.
- CVSS score range from 0.0 to 10.0.
  - Higher score indicating more severe vulnerabilities.

CVSS v3.x Ratings

Severity	Severity Score Range
None*	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

Challenges 1

- The process of updating the new vulnerability and assigning a score by NVD is very time-consuming.
  - The reported vulnerabilities in NVD all from previous version.

Challenges 1: No reported vulnerabilities on latest version

Open5gs : Security Vulnerabilities, CVEs,

Published in: 2024 January February March

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9 In CISA KEV Catalog

Sort Results By : Publish Date Update Date CVE Number CVE Number CVSS Score EPSS Score

Copy

CVE-2023-50020 An issue was discovered in open5gs v2.6.6. SIGPIPE can be used to crash AMF.	Max CVSS EPSS Score Published Updated	7.5 0.05% 2024-01-02 2024-01-11
CVE-2023-50019 An issue was discovered in open5gs v2.6.6. InitialUEMessage, Registration request sent at a specific time can crash AMF due to incorrect error handling of Nudm_UECM_Registration response.	Max CVSS EPSS Score Published Updated	5.9 0.05% 2024-01-02 2024-01-11
CVE-2023-23846 Due to insufficient length validation in the Open5GS GTP library versions prior to versions 2.4.13 and 2.5.7, when parsing extension headers in GPRS tunneling protocol (GPTv1-U) messages, a protocol payload with any extension header length set to zero causes an infinite loop. The affected process becomes immediately unresponsive, resulting in denial of service and excessive resource consumption. CVSS3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C	Max CVSS EPSS Score Published Updated	7.5 0.08% 2023-02-01 2023-02-08
CVE-2023-4885 Man in the Middle vulnerability, which could allow an attacker to intercept VNF (Virtual Network Function) communications resulting in the exposure of sensitive information.	Max CVSS EPSS Score Published Updated	6.5 0.09% 2023-10-03 2023-10-05

About

Open5GS is a C-language Open Source implementation for 5G Core and EPC, i.e. the core network of LTE/NR network (Release-17)

open5gs.org

core network lte epc 4g 3gpp 5g nr 5gc open5gs

Readme
AGPL-3.0 license
Activity
Custom properties
1.6k stars
102 watching
660 forks
Report repository

Releases 6

v2.7.0 Latest
on Dec 4, 2023

+ 5 releases

Challenges 2

- Different vulnerability scanning tools give different results.
  - False Negative: vulnerabilities are missed or not correctly identified
  - The two scanning instruments we have been utilising are a static analyser, and it may be necessary to incorporate a dynamic analyser.

Challenges 2: Result from Clair vs. Trivy: free5gc/amf

```
qwer3162@ubuntu18:~/Desktop/clair-scanner$ sudo ./clair-scanner --ip=172.17.0.1 free5gc/amf
2024/03/26 01:22:04 [INFO] ▶ Start clair-scanner
2024/03/26 01:22:05 [INFO] ▶ Server listening on port 9279
2024/03/26 01:22:05 [INFO] ▶ Analyzing c6e7bc72434f5a38f7684c8573b1d543e21564467ac46005caed4139e1fdb5cf
2024/03/26 01:22:05 [INFO] ▶ Analyzing 9ab13db2001674b9e9b8a6778da8a9ec3315df227fa7d3c7b12225aa4653ecaf
2024/03/26 01:22:05 [INFO] ▶ Analyzing 3aa0628f2e78533828c7bc24053cbf843a117e20f3130ce48ab036e056d1460f
2024/03/26 01:22:05 [INFO] ▶ Analyzing fcc6cb63964b4507a5868b1ecbfc1ac0617d7baf27bc7bb49a89d7230bb012b6
2024/03/26 01:22:05 [INFO] ▶ Analyzing 68abb53349c4667123402e3dd9dd4beb435b0c4deb01190005b637698a5b3159
2024/03/26 01:22:05 [INFO] ▶ Analyzing ad87e2be4405f5d8246cb23155e6b0d7bbde025c97fd95d77c5ce9ff3739863a
2024/03/26 01:22:05 [WARN] ▶ Image [free5gc/amf] contains 1 total vulnerabilities
2024/03/26 01:22:05 [ERRO] ▶ Image [free5gc/amf] contains 1 unapproved vulnerabilities
+------------+-------------------+-------------+-----------------+-------------------------------------------------------------------+
| STATUS     | CVE SEVERITY      | PACKAGE NAME | PACKAGE VERSION | CVE DESCRIPTION                                                   |
+------------+-------------------+-------------+-----------------+-------------------------------------------------------------------+
| Unapproved | Low CVE-2020-28928 | musl        | 1.2.2-r8        |                                                                   |
|            |                   |             |                 | https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-28928 |
+------------+-------------------+-------------+-----------------+-------------------------------------------------------------------+
```

Results from Clair

Result from Clair vs. Trivy: free5gc/amf

```
qwer3162@ubuntu18:~$ trivy image free5gc/amf
2024-03-26T01:22:49.790-0400    INFO    Vulnerability scanning is enabled
2024-03-26T01:22:49.790-0400    INFO    Secret scanning is enabled
2024-03-26T01:22:49.790-0400    INFO    If your scanning is slow, please try '--scanners vuln' to disable secret scanning
2024-03-26T01:22:49.790-0400    INFO    Please see also https://aquasecurity.github.io/trivy/v0.50/docs/scanner/secret/#recommendation for faster secret detection
2024-03-26T01:22:50.544-0400    INFO    Detected OS: alpine
2024-03-26T01:22:50.544-0400    INFO    Detecting Alpine vulnerabilities...
2024-03-26T01:22:50.547-0400    INFO    Number of language-specific files: 1
2024-03-26T01:22:50.547-0400    INFO    Detecting gobinary vulnerabilities...
2024-03-26T01:22:50.549-0400    WARN    version error ((devel)): malformed version: (devel)
2024-03-26T01:22:50.555-0400    WARN    This OS version is no longer supported by the distribution: alpine 3.15.11
2024-03-26T01:22:50.555-0400    WARN    The vulnerability detection may be insufficient because security updates are not provided

free5gc/amf (alpine 3.15.11)

Total: 0 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 0, CRITICAL: 0)


free5gc/amf (gobinary)

Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 1, HIGH: 0, CRITICAL: 0)

+---------------------------+-----------------+----------+--------+-------------------+---------------+--------------------------------------------------------------+
|          Library          | Vulnerability   | Severity | Status | Installed Version | Fixed Version |                            Title                             |
+---------------------------+-----------------+----------+--------+-------------------+---------------+--------------------------------------------------------------+
| google.golang.org/protobuf | CVE-2024-24786 | MEDIUM   | fixed  | v1.30.0           | 1.33.0        | golang-protobuf: encoding/protojson, internal/encoding/json: |
|                           |                 |          |        |                   |               | infinite loop in protojson.Unmarshal when unmarshaling       |
|                           |                 |          |        |                   |               | certain forms of...                                          |
|                           |                 |          |        |                   |               | https://avd.aquasec.com/nvd/cve-2024-24786                   |
+---------------------------+-----------------+----------+--------+-------------------+---------------+--------------------------------------------------------------+

/free5gc/cert/amf.key (secrets)

Total: 1 (UNKNOWN: 0, LOW: 0, MEDIUM: 0, HIGH: 1, CRITICAL: 0)

HIGH: AsymmetricPrivateKey (private-key)
================================================================================
Asymmetric Private Key
--------------------------------------------------------------------------------
 /free5gc/cert/amf.key:1 (added by 'COPY /free5gc/cert/amf.key ./cert/ # bui')
--------------------------------------------------------------------------------
   1 [ -----BEGIN RSA PRIVATE KEY-----**********************************************************************************************************************
**********************************************************************************************************************
**********************************************************************************************************************
**********************************************************************************************************************
**********************************************************************************************************************
**********************************************************************************************************************
**********************************************************************-----END RSA PRIVATE KEY-----
   2
================================================================================
```

Result from Trivy

Next Step

- Deploy Open5GS on an environment with the same configuration and compare the overhead of Open5GS core on the network metrics and compare it with Free5GC.
- VM deploy Free5GC and Open5GC, scan for vulnerabilities, and compare the results to the existing docker image vulnerability results.
- Use the attack graph to analyse the vulnerability results.
  - VM based Network Security Analyser: Mulval
  - Microservice Architecture: Breadth-First Search (BFS) approach to generate an attack graph based on the network topology

Thank You

Carleton University