Implementasi Dan Analisis Serangan Randsource DoS (Random Source Attack Denial of Service) Pada Jaringan 5G Prototype

1st Muhammad Rafi Firjatullah
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
fadhilahrafii@student.telkomuniversity.ac.id

2nd Rendy Munadi
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
rendymunadi@telkomuniversity.ac.id

3rd Fardan
Fakultas Teknik Elektro
Universitas Telkom
Bandung, Indonesia
fardanext@telkomuniversity.ac.id

***Abstrak* — 5G adalah generasi terbaru dari teknologi seluler untuk meningkatkan layanan dari generasi sebelumnya serta memiliki banyak fitur baru didalam sistem. Seiring perkembangan teknologi, terdapat program open source yang menyediakan layanan jaringan inti(core network)5G. Dengan program open source memungkinkan pengembang, peneliti atau industri untuk membentuk jaringan 5G itu sendiri atau dapat dikatakan privat seluler. Pada tugas akhir ini, penulis melakukan simulasi penyerangan terhadap jaringan 5G prototype berbasis open source yaitu open5gs. Pengujian dilakukan dengan menggunakan serangan Random source attack DoS (Denial of Service) pada 5G prototype dalam open source open5gs. Serangan yang dimaksud adalah dengan cara membanjiri alamat IP (Intetrnet Protocol) tertentu. Dengan demikian dapat mengetahui pengaruh serangan terhadap keamanan jaringan prototype yang telah dibuat. Berdasarkan hasil pengujian, terhadap jaringan prototype yang telah dibuat ketika mendapatkan serangan Randsource DoS memiliki dampak terhadap performansi jaringan di dalamnya. Server Open5gs mengalami peningkatan penggunaan CPU sebesar 98,6% dari kondisi normal atau sebelum terjadi penyerangan. Pada saat serangan berlangsung performansi QoS mengalami penurunan dari kondisi normal atau sebelum penyerangan.**

***Kata kunci*— Random Source Attack Denial of Service, Open5GS, Jaringan 5G Prototype**

I. PENDAHULUAN

Komunikasi seluler 5G lebih maju secara inovatif dibandingkan dengan seluler 4G komunikasi secara umum meliputi kecepatan, penggunaan protokol, dan konfigurasi jaringan. Jaringan 5G dikonfigurasi yang ditentukan oleh perangkat lunak dengan kecepatan 20 Gbps, 20 kali lebih cepat daripada evolusi sebelumnya (LTE), sementara jaringan inti 5G telah diubah dari tipe terpusat ke tipe desentralisasi untuk meminimalkan keterlambatan transmisi lalu lintas[1]. Karena perubahan teknis tersebut, ITU-R menetapkan layanan 5G. Mengklasifikasikan layanan 5G menjadi broadband seluler yang ditingkatkan di mana kecepatan adalah elemen terpenting, kemudian bandwidth adalah elemen kunci, dan minimalisasi waktu latensi yang diperlukan.

II. KAJIAN TEORI

A. Random Source Attack DoS (Denial of Service)

Random Source Attack DoS adalah membanjiri lalu lintas tertentu, dengan cara menghabiskan sumber daya (resource) yang dimiliki oleh perangkat tersebut sehingga mencegah user lain untuk memperoleh akses layanan yang diperoleh dari layanan tersebut. Serangan pada tugas akhir ini, bertujuan untuk menguji reaksi ketahanan system terhadap serangan lalu lintas dari sumber yang acak atau tidak diketahui. Pada serangan ini memiliki dampak yang terjadi pada jaringan prototype 5G dengan serangan Randsource-DoS adalah kepada gNB dari open5gs sehingga, gNB dari open5gs tidak mendapatkan sumber dari core sehingga layanan prototype 5G dari open source open5gs berhenti. Selain itu, dampak dari serangan ini berpengaruh terhadap pengiriman paket yang ditinjau dengan parameter QoS yaitu Throughput, Delay, Jitter dan Packet Loss

B. Open5GS

Open5gs merupakan software yang bertindak sebagai sisi core jaringan Open RAN. Open5gs adalah software open source dari bahasa pemrograman C yang diimplementasikan untuk 5G core dan EPC, yaitu core network dari gNB[2]. Open5gs digunakan untuk mengkonfigurasi jaringan SA yang bersifat private network sehingga dapat digunakan untuk kebutuhan percobaan dalam implementasi penyerangan.

C. Ueransim

Ueransim merupakan simulator open source untuk 5G EU dan 5G RAN (gNB). Sederhananya, Ueransim dapat menggantikan ponsel 5G secara efektif Ini memiliki fungsi mekanis yang sama[3]. komunikasi yang dapat dikendalikan Ueransim berisi antarmuka kontrol, yaitu komunikasi antara RAN dan AMF. Antarmuka pengguna, yaitu komunikasi antara RAN dan UPF, yaitu antarmuka radio Komunikasi antara UE dan RAN

III. METODE

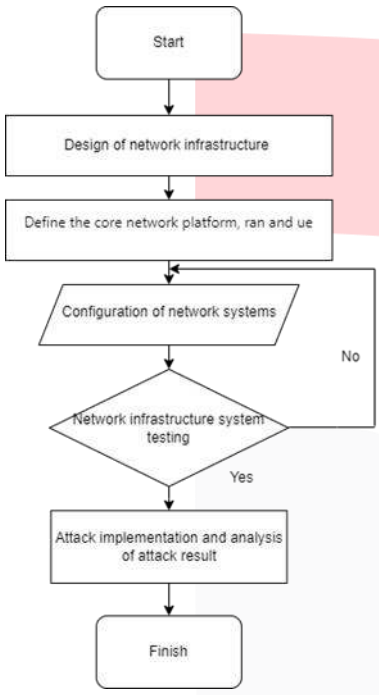
Metode penelitian pada tugas akhir ini dimulai dari melakukan desain system, desain simulasi yang akan digunakan sebagai jaringan prototype 5G, kemudian perangkat keras dengan minimum spesifikasi yang akan

digunakan, dan perangkat lunak yang digunakan, serta attack infrastruktur yang telah dilakukan.

Metode penelitian pada tugas akhir ini dimulai dari melakukan desain system, desain simulasi yang akan digunakan sebagai jaringan prototype 5G, kemudian perangkat keras dengan minimum spesifikasi yang akan digunakan, dan perangkat lunak yang digunakan, serta attack infrastruktur yang telah dilakukan.

A. Desain Sistem

Sebelum melakukan simulasi, dilakukan terlebih dahulu desain untuk system yang akan digunakan nantinya.



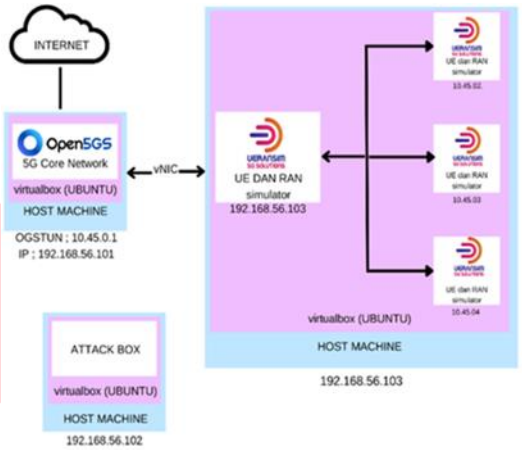
GAMBAR 1.
Flowchart Rencana Desain Sistem

Seperti pada gambar 1. Terdapat flowchart atau alur kerja sebelum dilakukan implementasi system yang sesungguhnya. Dapat dijelaskan pada flowchart yaitu,

1. Mendesain infrastruktur jaringan
2. Menentukan platform apa yang akan dipakai untuk Core Network, Ran dan UE.
3. Mengkonfigurasi sistem .
4. Pengujian sistem yang sudah dikonfigurasi, jika sudah berjalan dengan baik masuk ke tahap selanjutnya. Tetapi, jika masih terjadi kesalahan maka kembali ke tahap konfigurasi sistem.
5. Jika sistem Infrastruktur sudah berjalan masuk ke tahap implementasi penyerangan di sistem infrastruktur untuk mengambil data hasil penyerangannya dan dilakukan analisa terhadap penyerangan yang sudah diimplementasikan.
6. Selesai.

B. Desain Simulasi

Gambar dibawah merupakan model dari system yang akan dilakukan untuk pengujian penyerangan. Pada proses penulisan tugas akhir ini, penulis ingin melakukan penyerangan dengan menggunakan virtual mesin dari luar atau attacker untuk melakukan penyerangan dari Randsource DoS dari hping3. Kemudian, untuk perancangan system jaringan prototype 5G digunakan 3 virtual mesin yang berbeda untuk melakukan masing-masing model system penyerangan. Kemudian, sesuai pada gambar untuk core network, gNB dan UE ditempatkan pada tempat yang berbeda dan memiliki IP (Internet Protocol) yang berbeda juga.



GAMBAR 2.
Skema Infrastruktur Jaringan 5G

C. Perangkat Keras

Menurut rekomendasi dari open5gs Minimum spesifikasi yang digunakan[4]. Spesifikasi perangkat yang layak digunakan untuk simulasi berdasarkan minimum dan rekomendasinya adalah sebagai berikut

TABEL 1.
Minimum Spesifikasi yang Digunakan

Spesifikasi	Keterangan
Prosesor	Intel i3
RAM	4GB
HDD/SSD	256 GB
Ethernet	1 GB

Berdasarkan persyaratan minimum dan rekomendasi peralatan, spesifikasi berikut digunakan dalam tugas akhir ini, yang terkait dengan persyaratan minimum karena keterbatasan dalam hal produk yang tersedia.

TABEL 2.
Rekomendasi Spesifikasi yang Digunakan

Spesifikasi	Keterangan
Prosesor	Intel i10
RAM	16 GB
HDD/SSD	256 GB
Ethernet	1 GB

D. Perangkat Lunak

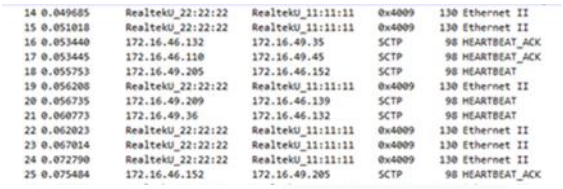
Selain perangkat keras, tentu juga membutuhkan perangkat lunak untuk menunjang implementasi jaringan

prototype 5G. berikut perangkat lunak yang diperlukan berdasarkan Open5gs dan Ueransim system requirement

1. Sistem operasi Ubuntu 22.04 LTS.
2. GCC version (4:11.2.0-1ubuntu1).
3. NodeJS 18.16.0-deb-1nodesource1.
4. Kernel version 5.19.0-45-generic.
5. VirtualBox 6.1.38_ubuntu r153438.

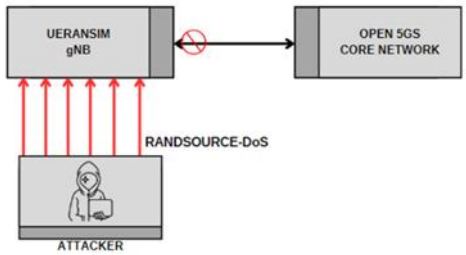
E. Attack Infrastructure Randsource DoS

Serangan Randsource adalah jenis lain dari serangan denial of service di mana server dibanjiri permintaan paket yang harus ditangani oleh mesin target. permintaan paket dalam jumlah besar dapat menghabiskan sumber daya dari server target, seperti CPU(Central Processing Unit) dan RAM(Random Access Memory)[5]. Dalam kasus penyerangan Randsource-DoS paket yang dikirimkan memiliki alamat IP(Internet Protocol) pengirim yang acak dan sulit untuk mengetahui dari mana serangan itu berasal. Pengujian DoS dalam simulasi jaringan 5G dimulai dengan mencari informasi tentang lalu lintas jaringan. Metode yang digunakan adalah pemantauan wireshark terhadap proses pensinyalan. Proses deteksi selama pensinyalan ditunjukkan pada gambar 4.



14	0.049685	RealtekU_22:22:22	RealtekU_11:11:11	0x4009	130 Ethernet II
15	0.051018	RealtekU_22:22:22	RealtekU_11:11:11	0x4009	130 Ethernet II
16	0.053440	172.16.46.132	172.16.49.35	SCTP	98 HEARTBEAT_ACK
17	0.053445	172.16.46.110	172.16.49.45	SCTP	98 HEARTBEAT_ACK
18	0.055753	172.16.49.205	172.16.46.152	SCTP	98 HEARTBEAT
19	0.056208	RealtekU_22:22:22	RealtekU_11:11:11	0x4009	130 Ethernet II
20	0.056735	172.16.49.209	172.16.46.139	SCTP	98 HEARTBEAT
21	0.060773	172.16.49.36	172.16.46.132	SCTP	98 HEARTBEAT
22	0.062023	RealtekU_22:22:22	RealtekU_11:11:11	0x4009	130 Ethernet II
23	0.067014	RealtekU_22:22:22	RealtekU_11:11:11	0x4009	130 Ethernet II
24	0.072790	RealtekU_22:22:22	RealtekU_11:11:11	0x4009	130 Ethernet II
25	0.075484	172.16.46.152	172.16.49.205	SCTP	98 HEARTBEAT_ACK

GAMBAR 1.
File PCAP Wireshark Lalu Lintas Jaringan



GAMBAR 4.
Skema Penyerangan Randsource DoS

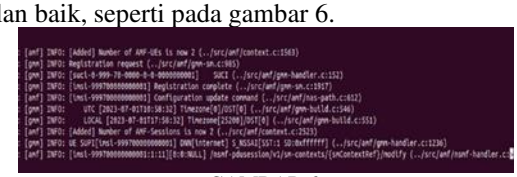
Hasil pengamatan melalui wireshark Gambar 4. Di atas menunjukkan bahwa wireshark mencatat semua hasil dari proses pensinyalan hingga pembuatan sesi PDU. Alamat IP node AMF, yang juga merupakan server host IP.

Pada gambar 5. Diatas menggambarkan skema dari penyerangan yang akan diimplementasikan, attacker atau penyerang berasal dari eksternal infrastruktur dengan virtual machine yang berbeda, penyerangan menuju gNB.

IV. HASIL DAN PEMBAHASAN

A. Pengujian Fungsionalitas Sistem

Pengujian fungsionalitas dilakukan untuk memastikan Core Network Open5GS dan UERANSIM dapat bekerja dan bisa berkomunikasi dengan baik. Pengujian dikatakan berhasil jika gNB dan UE UERANSIM bisa terhubung kepada Core Network Open5gs. Dan beberapa komponen Core Network Open5gs berfungsi seperti yang diharapkan. Simulasi Infrastruktur kami dijalankan oleh 2 buah virtual mesin, dan masing-masing viirtual mesin menggunakan sistem operasi ubuntu versi 22.04. Selain itu, dilakukan test atau pengujian komponen status open5gs-AMFD yang berjalan baik, seperti pada gambar 6.



GAMBAR 6.
Status Open5GS AMFD

Pada gambar 6. Dapat terlihat bahwa, komponen tersebut dapat berjalan dengan baik. Kemudian, dilakukan konfigurasi antara gNB dengan core network, seperti yang tertera pada gambar 7.

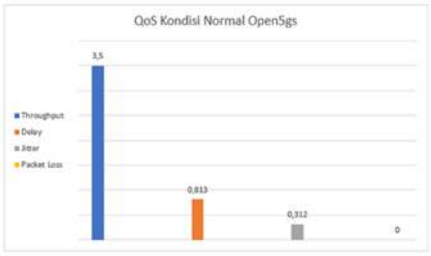
```
root@sys2-VirtualBox:/home/sys2/UERANSIM/config# ../build/nr-gnb -c gnb1.yaml
UERANSIM v3.2.6
[2023-07-24 18:53:44.218] [sctp] [info] Trying to establish SCTP connection... (192.168.56.101:38412)
[2023-07-24 18:53:44.277] [sctp] [info] SCTP connection established (192.168.56.101:38412)
[2023-07-24 18:53:44.277] [sctp] [debug] SCTP association setup ascId[3]
[2023-07-24 18:53:44.277] [ngap] [debug] Sending NG Setup Request
[2023-07-24 18:53:44.280] [ngap] [debug] NG Setup Response received
[2023-07-24 18:53:44.280] [ngap] [info] NG Setup procedure is successful
[2023-07-24 18:54:20.789] [rrc] [debug] UE[1] new signal detected
[2023-07-24 18:54:25.791] [rrc] [info] RRC Setup for UE[1]
[2023-07-24 18:54:25.792] [ngap] [debug] Initial NAS message received from UE[1]
[2023-07-24 18:54:25.864] [ngap] [debug] Initial Context Setup Request received
[2023-07-24 18:54:26.129] [ngap] [info] PDU session resource(s) setup for UE[1] count[1]
[2023-07-24 18:55:00.442] [rrc] [debug] UE[2] new signal detected
[2023-07-24 18:55:05.444] [rrc] [info] RRC Setup for UE[2]
[2023-07-24 18:55:05.445] [ngap] [debug] Initial NAS message received from UE[2]
[2023-07-24 18:55:05.495] [ngap] [debug] Initial Context Setup Request received
[2023-07-24 18:55:05.747] [ngap] [info] PDU session resource(s) setup for UE[2] count[1]
[2023-07-24 18:55:38.657] [rrc] [debug] UE[3] new signal detected
[2023-07-24 18:56:01.077] [rls] [debug] UE[3] signal lost
[2023-07-24 18:56:19.643] [rrc] [debug] UE[4] new signal detected
[2023-07-24 18:56:48.263] [rls] [debug] UE[4] signal lost
[2023-07-24 18:57:03.725] [rrc] [debug] UE[5] new signal detected
[2023-07-24 18:57:04.272] [rrc] [info] RRC Setup for UE[5]
[2023-07-24 18:57:04.273] [ngap] [debug] Initial NAS message received from UE[5]
[2023-07-24 18:57:04.323] [ngap] [debug] Initial Context Setup Request received
[2023-07-24 18:57:04.593] [ngap] [info] PDU session resource(s) setup for UE[5] count[1]
```

GAMBAR 7.
Status gNB Terhubung ke Core Network

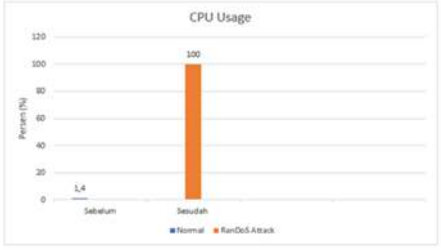
B. Pengujian Serangan Random Source Attack Denial of Service

Pada pengujian serangan Randsource, akan dilihat melalui performansi dari CPU Usage, Memory Usage, Throughput, Jitter, Delay, dan Packet Loss.

Sebelum dilakukan serangan menggunakan Randsource DoS, berikut adalah QoS dari kondisi Open5gs pada saat normal atau belum dilakukan penyerangan. Seperti dijelaskan pada gambar 10.



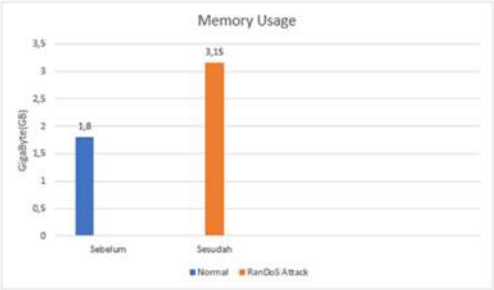
GAMBAR 10.
Kondisi Normal Open5GS



GAMBAR 11.
CPU Usage Sebelum dan Sesudah Penyerangan

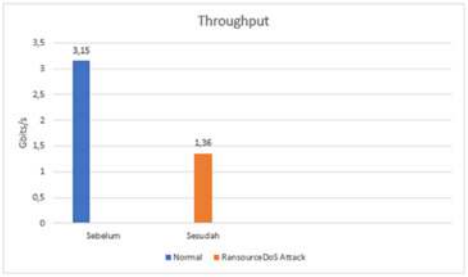
Kemudian, pada gambar 11. Menunjukkan kondisi CPU Usage setelah serangan, didapatkan bahwa kondisi sebelum

serangan kondisi CPU berada di angka 1,4%. Setelah dilakukan serangan meningkat menjadi 100%. Peningkatan yang signifikan ini menunjukkan bahwa serangan tersebut berhasil membebani sumber daya CPU dengan menghasilkan sejumlah besar paket yang memerlukan pemrosesan.



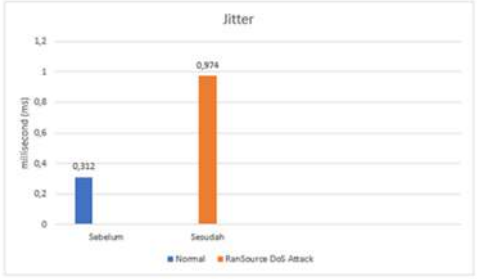
GAMBAR 12.
Memory Usage Sebelum dan Sesudah Penyerangan

Pada gambar 12. Menunjukkan kondisi dari memory usage sesudah serangan, didapatkan bahwa kondisi memory usage penggunaan memori sekitar 1,8 GB. Namun, setelah dilakukan serangan penggunaan memori menjadi 3,15 GB. Hal ini menandakan bahwa serangan Randsource DoS menyebabkan peningkatan pemakaian memori karena sistem harus mengelola lebih banyak paket dan beban kerja yang lebih berat.



GAMBAR 13.
Throughput Sebelum dan Sesudah Penyerangan

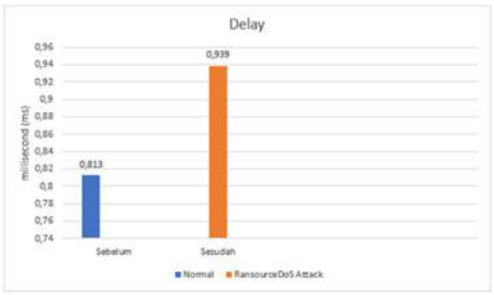
Pada throughput, seperti dijelaskan pada gambar 13. Menunjukkan bahwa setelah serangan, throughput menurun menjadi 1,36 Gbps, yang dimana sebelum serangan throughput system mencapai 3,15 Gbps. Hal ini mengindikasikan bahwa serangan DoS randsource attack mampu mengganggu aliran data yang melewati infrastruktur 5G, sehingga mengurangi kemampuan sistem dalam mengirimkan dan menerima data dengan efisiensi yang sama seperti sebelum serangan



GAMBAR 14.
Packet Loss Sebelum dan Sesudah Penyerangan

Pada gambar 14. Menunjukkan kondisi dari packet loss sebelum dan sesudah dilakukan penyerang menggunakan Randsource DoS, didapatkan bahwa packet loss tetap di angka 0. Hal ini dapat terjadi, dikarenakan kemampuan infrastruktur 5G dalam meminimalisir packet loss tidak hilang.

Pada gambar 15. Menunjukkan kondisi dari delay sesudah serangan, menunjukkan mengalami peningkatan delay menjadi 0,939 ms. Dibandingkan dari kondisi sebelum dilakukan serangan yaitu 0,813 ms. Hal ini ini mengindikasikan adanya penundaan dalam pengiriman paket data, mungkin disebabkan oleh beban kerja tambahan yang dihasilkan oleh serangan. Namun, nilai peningkatan packet delay tetap dalam batas yang dapat diterima dan mungkin tidak signifikan bagi penggunaan layanan yang lebih umum



GAMBAR 16.
Jitter Sebelum dan Sesudah Penyerangan

Pada gambar 16. Dijelaskan bahwa kondisi setelah dilakukan serangan, jitter meningkat menjadi 0,974 ms, sebelum dilakukan serangan jitter berada di angka 0,312 ms. Peningkatan ini mengindikasikan variasi yang lebih tinggi dalam waktu pengiriman paket data, mungkin disebabkan oleh fluktuasi dalam penggunaan sumber daya akibat serangan Randsource DoS. Meskipun demikian, nilai jitter yang masih dalam rentang yang dapat diterima mungkin tidak akan memiliki dampak yang besar pada layanan yang lebih umum.

V. KESIMPULAN

Setelah dilakukan pengujian dari serangan Randsource DoS(Denial of Service) pada jaringan 5G prototype, didapatkan bahwa serangan ini akan mematikan layanan, dikarenakan server akan dibanjiri permintaan paket kepada virtual mesin. Pada serangan ini dapat dilihat bahwa performansi dari CPU Usage, Memory Usage, Throughput, Packet Loss, Delay dan Jitter. Semuanya mengalami penurunan performansi yang cukup signifikan, hal ini dapat dikatakan bahwa serangan tersebut berhasil untuk membuat infrastruktur dari 5G prototype tidak dapat bekerja secara optimal dan maksimal seperti pada normalnya.

REFERENSI

[1] International Telecommunication Union Radiocommunication. Detailed Specifications of the Terrestrial Radio Interfaces of International Mobile Telecommunications-2020 (2020)

[2] Damayanti dkk. (2022). Desain and Build 4G Open Radio Access Network at SmartLab Politeknik Negeri Jakarta. Doi: 10.31289/jite.v6i2.7537

[3] github.com. (2022, 13 Januari). Aligungr/UERANSIM. Diakses pada 22 Juli 2023, dari https://github.com/aligungr/UERANSIM

[4] Open5gs.org. (2022, 18 Juni). https://open5gs.org/. Diakses pada 22 Juli 2023, dari https://open5gs.org/open5gs/docs/tutorial/01-your-first-lte/

[5] Pande, S., Khamparia, A., Gupta, D., and Thanh, D.N. DDOS Detection using Machine Learning Technique. In Recent Studies on Computational Intelligence, pp. 59-68, 2021.