BAB 1
USULAN GAGASAN

1.1 Latar Belakang Masalah

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.

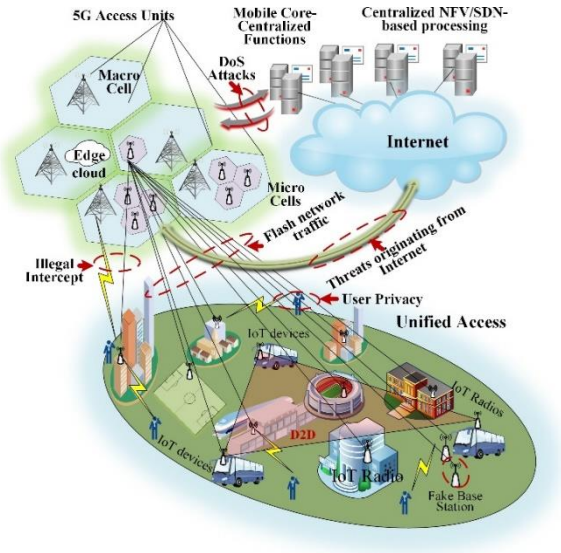
1.2 Informasi Pendukung Masalah

Perkembangan Generasi Kelima (5G) adalah suatu jaringan nirkabel untuk menghubungkan hampir semua aspek kehidupan melalui jaringan dengan kecepatan yang jauh lebih tinggi, dengan latensi sangat rendah dan konektivitas di mana-mana. Sebuah infrastruktur jaringan harus membuat penggunanya merasa aman dari segi komponen, dan layanan[2]. Aspek ancaman keamanan 5G telah berkembang sangat besar karena peningkatan jenis layanan yang belum pernah terjadi sebelumnya dan dalam jumlah penambahan perangkat. Oleh karena itu, solusi keamanan jika tidak dikembangkan harus sudah dibayangkan untuk mengatasi berbagai ancaman pada berbagai layanan, teknologi baru, dan peningkatan informasi pengguna yang dapat diakses oleh jaringan [3].

5G tidak hanya membutuhkan keamanan saluran komunikasi yang tepat untuk mencegah ancaman keamanan yang teridentifikasi, tetapi juga untuk memelihara programabilitas dan visibilitas status jaringan global. IPsec adalah protokol keamanan yang paling umum digunakan untuk mengamankan saluran komunikasi di jaringan telekomunikasi saat ini seperti 4G-LTE

Sistem komunikasi nirkabel telah rentan terhadap kerentanan keamanan sejak awal. Di jaringan nirkabel generasi pertama (1G), ponsel dan saluran nirkabel ditargetkan untuk kloning ilegal dan menyamar. Pada generasi kedua (2G) nirkabel jaringan, spam pesan menjadi umum tidak hanya untuk serangan meluas tetapi menyuntikkan informasi palsu atau menyiarkan informasi pemasaran yang tidak diinginkan. Pada generasi ketiga (3G) jaringan nirkabel, komunikasi berbasis IP memungkinkan migrasi kerentanan dan tantangan keamanan Internet di domain nirkabel. Dengan meningkatnya kebutuhan berbasis IP komunikasi, jaringan seluler Generasi keempat (4G). memungkinkan proliferasi perangkat pintar, lalu lintas multimedia, dan layanan baru ke dalam domain seluler [4]

Langkah penting dalam memfasilitasi jaringan yang sehat adalah memantau dan menganalisis lalu lintas persinyalan ketika melintasi perbatasan jaringan, yang memungkinkan untuk menangkap kesalahan konfigurasi dan suguhan potensial. Untuk memiliki implementasi yang sukses dari fitur keamanan ini, operasi jaringan perlu digunakan sistem deteksi ancaman khusus yang menganalisis lalu lintas secara nyata waktu. Untuk dapat memblokir aktivitas jahat secara real time tanpa memiliki dampak dramatis pada jaringan situasi yang ideal[5]



Gambar 1.1 Mengenai Ancaman pada 5G[5]

Dalam melakukan penetrasi terhadap infrastruktur jaringan 5G ada beberapa macam pemodelan serangan yang bisa di pakai dan penyebab serangan tersebut terjadi yaitu.

1. Denial of Service (DoS) attacks on the infrastructure:
   Elemen kontrol jaringan yang terbuka, dan saluran kontrol tidak dienkripsi.
2. User Plane Integrity:
   Tidak ada perlindungan berbasis kriptografi untuk data pengguna.
3. Signaling storms:
   Non-Access Stratum (NAS) lapisan Third Generation Partnership Project (3GPP).

1.3 Analisis Umum

1.3.1 Rumusan Masalah

1. Terdapat Ancaman keamanan pada infrastruktur 5G, Dimana dampak tersebut sangat besar untuk publik.
2. Pengetahuan yang kurang tentang pola dan cara kerja serangan pada jaringan 5G.
3. Sulit menemukan platform yang bisa digunakan untuk melakukan pemodelan validasi serangan.

1.3.2 Tujuan

1. Mengurangi dampak dan mampu mendeteksi keamanan pada infrastruktur jaringan 5G.
2. Mendapatkan pengetahuan yang utuh tentang pola dan cara kerja serangan pada jaringan 5G.
3. Membuat platform untuk mendapatkan informasi tentang model dan cara kerja serangan termasuk untuk memvalidasi serangan tersebut.

1.3.3 Batasan Masalah

Adapun Batasan masalah dalam penelitian ini untuk memperjelas yaitu:

1. Implementasi berupa simulasi menggunakan virtual mesin pada virtualbox.
2. Arsitektur yang digunakan pada penelitian ini yaitu jaringan 5G Stand Alone.
3. Layanan 5G *core network service* yang digunakan yaitu adalah Open5gs.
4. Perangkat lunak *open source m*eliputi RAN dan client menggunakan simulator UERANSIM.
5. Percobaan pengujian keamanan berupa serangan Random Source Attack Denial of Service(DoS).
6. Percobaan pengujian keamanan berupa serangan Fuzzing dilakukan pada mesin virtual server Open5gs.

1.4 Kebutuhan yang Harus Dipenuhi

Berdasarkan analisis yang telah dilakukan, kebutuhan yang diperlukan pada penelitian ini yaitu:

1.4.1 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[6]. Open5gs digunakan untuk mengkonfigurasi jaringan SA (*Stand Alone*) yang bersifat private network sehingga dapat digunakan untuk kebutuhan percobaan dalam implementasi penyerangan.

1.4.2 UERANSIM

Ueransim adalah adalah simulator open source untuk 5G EU dan 5G RAN (gNB). Sederhananya, ueransim dapat menggantikan ponsel 5G secara efektif Ini memiliki fungsi mekanis yang sama[7]. 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.

1.4.3 Wireshark

Wireshark adalah perangkat lunak analisis jaringan yang memungkinkan pengguna merekam dan menganalisis lalu lintas jaringan secara real time[8]. Wireshark dapat digunakan untuk memecahkan masalah jaringan, mengidentifikasi intrusi, mengoptimalkan kinerja jaringan, dan bahkan memecahkan masalah keamanan

1.5 Solusi Sistem yang Diusulkan

1.5.1 Karakteristik sistem

Berdasarkan dari latar belakang, permasalahan dan tujuan yang sudah dijabarkan maka ditentukan tiga solusi sistem yang ditawarkan yaitu:

1. Perancangan core network dalam simulator Open5gs
2. Perancangan infrastruktur 5G dalam open source UERANSIM
3. Analisis hasil pengukuran Quality of Service(QoS) dalam Wireshark

1.5.1.1 Perancangan core network dalam simulator Open5GS

Pada perancangan core network, 5G core network memiliki tugas sebagai *mobility management, session management, authentication* dan *security.*

1.5.1.2 Perancangan infrastruktur 5G dalam open source UERANSIM

Pada perancangan infrastruktur 5G, ueransim digunakan sebagai pengganti ponsel 5G secara virtual. Ueransim memiliki fungsi antara lain sebagai *Control Interface* yaitu sebagai komunikasi antara *Radio Access Network*(RAN) dan *Access and Mobility Management Function*(AMF), selain itu sebagai User Interface yaitu berfungsi untuk komunikasi antara *Radio Access Network*(RAN) dan *User Plane Function*(UPF), selain itu terdapat Radio Interface sebagai komunikasi antara *User Equipment*(UE) dan *Radio Access Network*(RAN).

1.5.1.3 Analisis hasil pengukuran Quality of Service (QoS) dalam Wireshark

Pada hasil pengukuran quality of service, setelah dilakukan penyerangan menggunakan serangan Random source Denial of Service(DoS) dan Fuzzing, maka didapatkan hasil pcap dalam wireshark. Kemudian, digunakan tools iperf3 untuk menghitung dan analisis seperti hasil Throughput, Jitter, Packet Loss, dan Delay.

1.5.2 Metode Penelitian

1. Studi Literatur

   Materi pembelajaran dari sumber referensi seperti buku, artikel, dan Internet mengenai 5G, arsitektur inti 5G, dan keamanan 5G.

2. Perancangan Sistem

   Mengidentifikasi masalah dan merancang arsitektur jaringan yang akan digunakan untuk membangun sistem dengan Open5gs.

3. Simulasi dan Implementasi

   Menerapkan desain sistem dan hasil pengujian yang sebelumnya telah dibuat.

4. Analisis Hasil Penguujian

   Melakukan analisa dari hasil yang telah didapatkan sesuai dengan tujuan system yang telah ditentukan.

5. Pembuatan Laporan

   Menyusun laporan dari proses perancangan desain system hingga melakukan analisis kemudian dimuat dalam bentuk buku.

1.6 Kesimpulan dan Ringkasan CD-1

5G merupakan teknologi jaringan seluler kelima yang menawarkan kecepatan data yang lebih tinggi dan latensi yang lebih rendah dibandingkan dengan teknologi seluler sebelumnya. Namun, seperti teknologi jaringan lainnya, 5G juga memiliki beberapa ancaman yang perlu diperhatikan. Maka, kesimpulan dari dokumen ini adalah akan dilakukan implementasi 5G infrastruktur yang akan digunakan untuk pemodelan serangan keamanan. Hasil pemodelan dapat digunakan sebagai informasi untuk mengetahui bagaimana serangan bekerja, dampaknya terhadap jaringan serta dapat diketahui kemudian cara untuk menanganinya atau mencegahnya.