# Implementasi Wireless Intrution Detection System melalui Teknik Pemindaian pada Seluler

1st Fabhian Aliy Rajaie kamil
*Fakultas Teknik Elektro*
*Universitas Telkom*
Bandung, Indonesia
fabhianaliy@student.telkomuniversity.ac.id

2nd Ida Wahidah Hamzah
*Fakultas Teknik Elektro*
*Universitas Telkom*
Bandung, Indonesia
wahidah@telkomuniversity.ac.id

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

***Abstrak*** **—— Penelitian ini membahas penerapan Wireless Intrusion Detection System (WIDS) dalam jaringan GSM (2G) dan LTE (4G) dengan tujuan meningkatkan keamanan komunikasi seluler. Dengan semakin kompleksnya ancaman keamanan dalam era komunikasi nirkabel, penerapan WIDS menjadi sangat relevan untuk mendeteksi aktivitas mencurigakan dan potensi serangan. Dua teknik pemindaian digunakan dalam penelitian ini: gr-gsm untuk jaringan GSM dan CellSearch untuk jaringan LTE. Pengumpulan data hasil pemindaian diintegrasikan dengan skrip Python untuk penyimpanan data dalam sebuah database.**

**Hasil penelitian mengungkapkan bahwa penerapan WIDS mampu mendeteksi potensi serangan dalam jaringan GSM dan LTE. Teknik gr-gsm efektif dalam menganalisis sinyal GSM menggunakan perangkat lunak sumber terbuka, sedangkan teknik CellSearch berhasil mengidentifikasi sel atau stasiun pangkalan dalam jaringan LTE. Hasil pemindaian disimpan dalam database melalui skrip Python, memberikan wawasan yang penting untuk evaluasi keamanan dan analisis data.**

**Penelitian ini menegaskan pentingnya WIDS dalam melindungi jaringan seluler dari serangan-spionase dan pelanggaran keamanan. Lebih lanjut, penelitian ini mengindikasikan potensi pengembangan lebih lanjut dalam penggunaan teknik pemindaian dan analisis data untuk menghadapi tantangan keamanan yang terus berkembang dalam komunikasi nirkabel modern. Dengan demikian, penelitian ini memberikan kontribusi penting dalam mendukung integritas dan keamanan sistem komunikasi seluler di era teknologi yang terus maju.**

***Kata Kunci:*** **Wireless Intrution Detection System, Keamanan Jaringan Seluler, Pemindaian.**

***Abstract -This research discusses the implementation of Wireless Intrusion Detection System (WIDS) in GSM (2G) and LTE (4G) networks with the aim of improving mobile communication security. With the increasing complexity of security threats in the era of wireless communications, the implementation of WIDS becomes highly relevant to detect suspicious activities and potential attacks. Two scanning techniques are used in this research: gr-gsm for GSM networks and CellSearch for LTE networks. Data collection of scan results is integrated with Python scripts for data storage in a database.***

***The results revealed that the application of WIDS is able to detect potential attacks in GSM and LTE networks. The gr-gsm technique is effective in analysing GSM signals using open source software, while the CellSearch technique successfully identifies cells or base stations in LTE networks. The scan results are stored in a database via Python scripts, providing important insights for security evaluation and data analysis.***

***This research confirms the importance of WIDS in protecting mobile networks from espionage attacks and security breaches. Furthermore, this research indicates the potential for further development in the use of scanning and data analysis techniques to deal with the ever-growing security challenges in modern wireless communications. As such, this research makes an important contribution in supporting the integrity and security of mobile communication systems in an era of ever-advancing technology.***

***Keywords: Wireless Intrusion Detection System, Mobile Network Security, Scanning..***

## I. PENDAHULUAN

Inovasi telah membawa kemajuan yang sangat penting, terutama dalam korespondensi jarak jauh dan portabel. Meskipun demikian, kemajuan ini juga tetap terkait erat dengan perluasan serangan, misalnya, pengawasan, yang merusak keamanan data dan organisasi. Untuk mengatasi hal ini, Kerangka Kerja Penemuan Gangguan Jarak Jauh (WIDS) muncul sebagai pengaturan yang signifikan, yang memberdayakan pengenalan dini terhadap latihan yang meragukan.

Fokus dari penelitian ini adalah bagaimana WIDS dapat digunakan dalam komunikasi seluler. Penelitian ini menyelidiki penerapan pemindaianstasiun pangkalan untuk mendeteksi ancaman spionase pada frekuensi 2G dan 4G. Pemeriksaan ini bertujuan untuk mengembangkan keamanan lebih lanjut dengan membedakan tindakan yang meragukan dalam organisasi yang serbaguna.

Penelitian ini diantisipasi untuk memberikankontribusi pada ancaman spionase yang semakin kompleks dengan mendapatkan pemahamantentang masalah keamanan yang terkait dengan komunikasi seluler dan fungsi WIDS. Di era teknologi modern, solusi ini diharapkan dapat mendorong terciptanya sistem keamanan yang lebih kuat untuk menjaga integritas komunikasi seluler.

## II. KAJIAN TEORI

Sinyal seluler, atau disebut juga tanda ponsel atau sinyal jaringan, mengacu pada gelombang elektromagnetik yang digunakan oleh ponsel untuk berbicara dengan jaringan seluler. Hal ini memungkinkan kita untuk melakukan panggilan suara, mengirim pesan instan, mengakses web, dan menggunakan aplikasi yang berbeda. Di Indonesia, terdapat dua klasifikasi: resmi dan tidak berlisensi. Untuk klasifikasi resmi, Band 1 berada di 2.100 MHz, Band 3 di 1.800 MHz, Band 5 di 800 MHz,
Band 8 di 900 MHz, serta Band 31 di 450 MHz dan Band 40 di 2.300 MHz. Sementara itu, untuk kelas tidak berizin ada di 2,4 GHz, 5,8 GHz dan di ruang lingkup 919-925 MHz yang masih dalam proses survei karena diperkirakan akan menghalangi aktivitas di organisasi seluler[1].

### A. Jaringan GSM

Teknologi komunikasi seluler digital yang dikenal sebagai *Global System for Mobile Communication* (GSM, yang awalnya merupakan singkatan dari Groupe Spécial Mobile). Teknologi GSM digunakan secara luas dalam komunikasi seluler, khususnya pada ponsel. Untuk menjamin bahwa sinyal informasi yang dikirim akan sampai ke tujuan, teknologi ini memanfaatkan gelombang mikro dan transmisi sinyal pembagian waktu. GSM digunakan sebagai norma di seluruh dunia untuk korespondensi serbaguna serta inovasi portabel yang paling luas di dunia ini[2].

### B. Jaringan LTE

*Long Term Evolution* (LTE) adalah nama yang diberikan untuk sebuah proyek oleh Proyek Kemitraan Generasi Ketiga (3GPP). Teknologi ini adalah teknologi pra-4G yang ditentukan dalam standar 3GPP Release 8[3]. Proyek ini mencerminkan upaya kolektif dalam mewujudkan inovasi telekomunikasi yang bertujuan meningkatkan efisiensi jaringan, throughput data yang lebih tinggi, dan kemampuan manajemen lalu lintas yang ditingkatkan,

## III. METODE

Metode penelitian dalam tugas akhir ini dimulai dari melakukan rencana kerangka kerja, rencana simulasi yang akan digunakan sebagai pemindaian pada jaringan seluler, kemudian perangkat keras dengan spesifikasi yang akan digunakan, dan perangkat lunak yang digunakan.

### A. Desain Sistem

Sebelum melakukan simulasi, terlebih dahulu dilakukan perencanaan terhadap kerangka kerjayang akan digunakan nantinya.

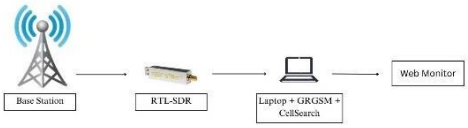

GAMBAR 3. 1
Flowchart Rencana Desain Sistem

Seperti pada gambar diatas, terdapat flowchart atau alur kerja sebelum dilakukan implementasi sstem yang sesungguhnya.

### B. Desain Simulasi

Gambar dibawah merupakan model dari system

yang akan dilakukan pada pemindaian jaringanseluler




GAMBAR 3. 2
Skema Implementasi

Penulis akan melaksanakan pemindaian pada jaringan 2G dan 4G dengan memanfaatkan perangkat keras rtl-sdr. Data yang diperoleh dari hasil pemindaian ini akan diarsipkan dalam basis data pemantauan web melalui implementasi skrip yang telah diadaptasi.

C. Pemindaian Jaringan Seluler

Pada penelitian ini, dilakukan pemindaian pada dua jenis frekuensi, yakni 2G dan 4G, dalam konteks jaringan seluler. Untuk pemindaian pada jaringan 2G (GSM), digunakan teknik gr-gsm, sebuah perangkat lunak sumber terbuka yang dirancang khusus untuk menangani sinyal dalam komunikasi portabel, terutama dalam konteks jaringan GSM (2G). Fungsi utama dari GR-GSM adalah untuk melakukan proses penyaringan, analisis, dan interpretasi sinyal GSM yang diterima melalui perangkat radio, seperti perangkat definisi peralatan radio atau SDR (Software Defined Radio).

Sementara itu, pemindaian pada jaringan 4G (LTE) menggunakan teknik CellSearch. Teknik ini bertujuan untuk mengidentifikasi dan menemukan sel atau stasiun pangkalan yang dapat diakses dalam jangkauan ponsel. Dengan demikian, melalui pendekatan yang berbeda pada pemindaian frekuensi 2G dan 4G, penelitian ini mengamati penggunaan teknik gr-gsm dan CellSearch dalam menghadapi kebutuhan deteksi pada kedua jenis jaringan seluler tersebut.

D. Menyimpan data pada database

Setelah menyelesaikan pemeriksaan dengan menggunakan metode gr-gsm dan CellSearch pada jaringan 2G dan 4G, tahap berikutnya dalam penelitian ini adalah menyimpan hasil informasi yang didapat ke dalam kumpulan data. Skrip Python yang dibuat untuk menyimpan dan mengelola data hasil pemindaian digunakan untuk mencapai tujuan pada penelitian ini.

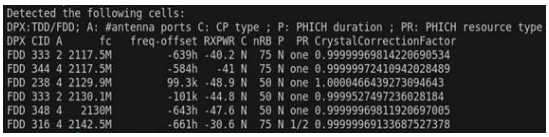
## IV. HASIL DAN PEMBAHASAN

A. Pengujian Fungsionalitas Sistem

Pengujian fungsionalitas dilakukan untuk memastikan rtl-sdr dapat menjalankan GR-GSM dan CellSearch dengan baik. Pengujian dikatakan berhasil jika rtl-sdr dapat memindai jaringan 2G dan 4G. Dan dapat menampilkan hasil menggunakan kedua teknik tersebut. Simulasi Infrastruktur dijalankan oleh sebuah virtual mesin yaitu, sistem operasi Dragon Focal. Selain itu, dilakukan pengujian *Quality of Service* terhadap kedua jaringan tersebut.

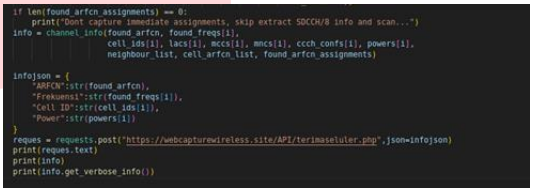

GAMBAR 4. 1
Hasil pemindaian dengan teknik GR-GSM

Pada gambar diatas dapat terlihat bahwa, rtl-sdr berjalan dengan baik, dan menampilkan data yang didapat menggunakan gr-gsm pada jaringan 2G.

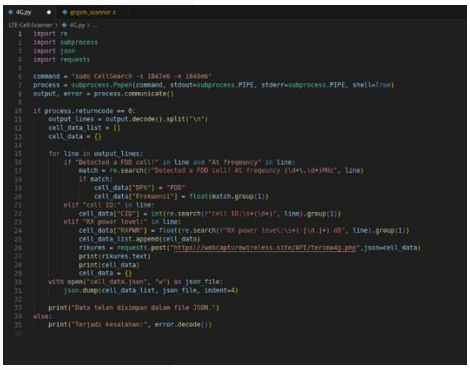



GAMBAR 4. 2
Hasil Pemindaian dengan Teknik CellSearch

Pada gambar diatas dapat terlihat bahwa rtl-sdr juga bekerja dengan baik dan dapat menampilkan data yang diapat menggunakan teknik CellSearch. Dengan berhasilnya pemindaian pada kedua jaringan tersebut Langkah berikutnya adalah menjalankan skrip python yang telah dibuat agar dapat mengirimkan hasil data kepada database.



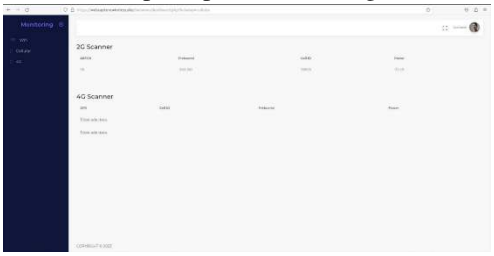

GAMBAR 4. 3
Skirp Python untuk GR-GSM



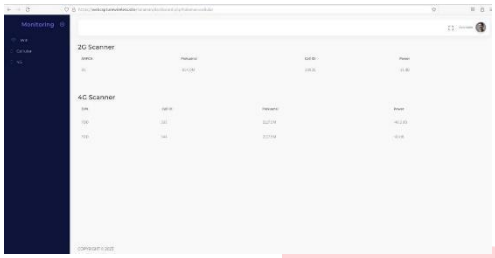

GAMBAR 4. 4
Skrip Python untuk CellSearch

Melalui penerapan perangkat penerimaan Nooelec NESDR SMArTee XTR, data yang berhasil tercatat kemudian diolah menggunakan skrip Python yang telah dirancang khusus. Data ini diubah menjadi format json yang memiliki struktur terorganisir. Tujuan dari langkah ini adalah untuk memungkinkan unggahan dan visualisasi data

melalui sebuah platform pemantauan berbasis web. Berikut adalah tampilan pada monitoring web:



GAMBAR 4. 5
Tampilan web Hasil Pemindaian GSM



GAMBAR 4. 6
Tampilan web Hasil Pemindaian LTE

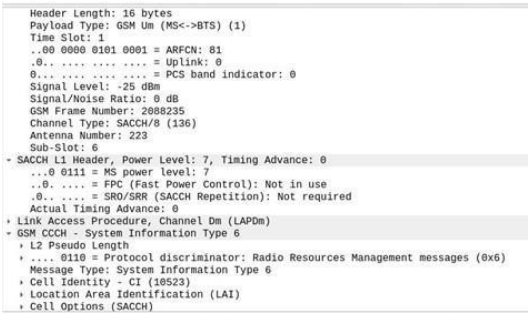
B. Pengujian Quality of Service

Setelah mengimplementasikan pemindaian pada jaringan 2G dan 4G, penulis melakukan pengujian pengukuran nilai TA pada jaringan 2G, sedangkan pda jaringan 4G dilakukan pengukuran pada nilai RSRP dan RSSI, TA (*Timing Advance)* digunakan untuk menunjukkan seberapa jauh jarak MS (Mobile Station) dari BS (Base Station) [4], [5]. Nilai TA juga akan sebanding dengan waktu yang dibutuhkan BTS untuk menerima sinyal yangdikirimkan oleh MS. Karena jarak antara MS dan BTS berbeda, waktu di mana MS diizinkan untuk mengirimkan sinyal ke BTS dalam slot waktu harus ditentukan dengan tepat[5].

Sedangkan RSRP (*Reference Signal Received Power*) adalah power dari sinyal yang di terima dari eNodeB ke UE. Pada teknologi 2G parameter ini bisa dianalogikan RxLevel, sedangkan pada 3G sebagai RSCP, dan RSSI (Received Signal Strength Indicator) merupakan parameter yang menyatakan keseluruhan daya sinyal yang diterima oleh user dalam satuan dBm[3].

1. Timing Advance

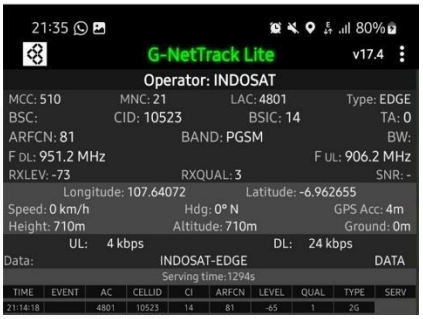
Untuk mencari nilai TA, kami menggunakan perangkat lunak paket analisis yaitu Wireshark, dengan cara mengaplikasikan filter *Timing Advance* seperti gambar berikut:



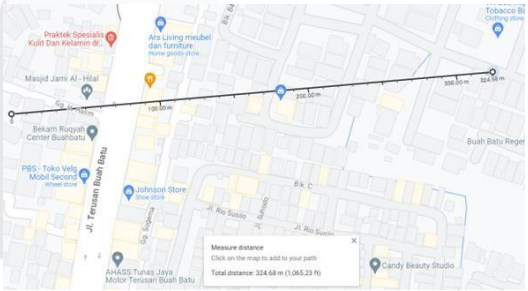

GAMBAR 5. 1
Nilai TA pada Wireshark

Pada gambar diatas, ditemukan bahwa sinyal TA = 0, *timing advance* ditransmisikan dalam SACCH sebagai angka antara 0 dan 63, dalam satuan periode bit (3,69 mikrodetik). Jika sebuah sinyal bergerak dengan kecepatan 300 meter per mikrodetik (kecepatan cahaya), masing-masing TA akan berjarak sekitar 1100 m (meter). Karena merupakan jarak melingkar, setiap kenaikan nilai TA sesuai dengan jarak 550 m antara *mobile station* dan *BTS*.

Misalnya, TA = 0 berarti ponsel berjarak 0 m hingga 550 m dari stasiun, TA=1 berarti 550 m- 1100 m, TA=2 berarti 1100 m-1650 m, dan seterusnya. Tahapan selanjutnya, peneliti menggunakan aplikasi *mobile* yaitu, *G-NetTrack Lite* dan *Google maps* guna memvalidasi nilai TA= 0 (0m-550m) antara *mobile station* dengan *base station*:




GAMBAR 5. 2
Nilai TA pada Aplikasi G-NetTrack Lite

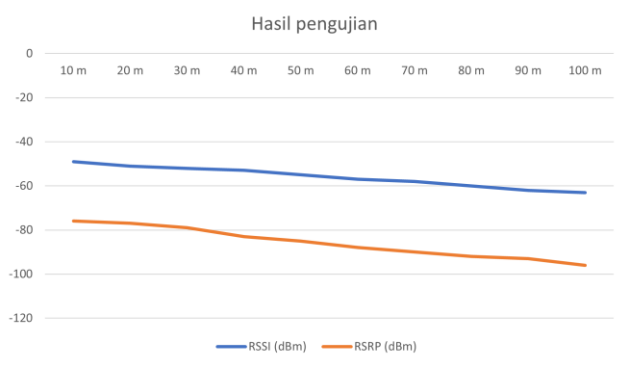



GAMBAR 5. 3
Jarak antara Base Station dengan MobileStation

2. RSRP dan RSSI

Dalam pengujian ini, digunakan aplikasi mobile devices yang disebut CellMapper untuk memonitor dan menganalisis kualitas sinyal

jaringan LTE pada frekuensi yang ditentukan. Aplikasi CellMapper memberikan data mengenai nilai RSRP dan RSSI serta titik koordinat dari base station yang terhubung, peneliti melakukan pengujian pada jarak dari 10 meter hingga 100 meter, dan didapatkan hasil seperti berikut:




GAMBAR 5. 4
Grafik Pengujian Nilai RSRP dan RSSI pada Jarak 100 meter

## V. KESIMPULAN

1. Efektivitas Deteksi Intrusi

Penelitian ini menunjukkan bahwa penerapan WIDS dalam jaringan GSM dan LTE memiliki potensi yang signifikan dalam mendeteksi aktivitas mencurigakan dan serangan potensial. Metode pemindaian seperti gr-gsm dan CellSearch membantu mengidentifikasi perangkat atau aktivitas yang tidak sah dalam jaringan, sehingga meningkatkan keamanan dan integritas komunikasi seluler.

2. Relevansi Terhadap Keamanan:

Dengan semakin kompleksnya ancaman terhadap keamanan jaringan seluler, implementasi WIDS menjadi semakin penting. Penelitian ini mengkonfirmasi bahwa WIDS memiliki peran penting dalam mengatasi serangan-spionase dan pelanggaran keamanan dalam jaringan GSM dan LTE.

3. Potensi Pengembangan Lanjutan

Penelitian ini membuka pintu bagi pengembangan lanjutan dalam penggunaan WIDS pada jaringan seluler. Lebih banyak teknik pemindaian, analisis lebih mendalam, dan integrasi dengan teknologi baru dapat meningkatkan kemampuan WIDS dalam mendeteksi serangan berbasis nirkabel.

Dengan demikian, penelitian ini menegaskan peran kritis WIDS dalam meningkatkan keamanan jaringan GSM dan LTE, dan memberikan landasan untuk pengembangan lebih lanjut dalam domain ini guna menghadapi tantangan keamanan yang semakin berkembang dalam era komunikasi nirkabel modern.

## REFERENSI

[1] M. Hadiyana, “Spektrum Frekuensi dan Standar IoT Dirilis Tahun Ini,” Aug. 29, 2018. https://www.kominfo.go.id/content/detail/14110/spektrum-frekuensi-dan-standar-iot-dirilis-tahun-ini/0/sorotan_media (accessed Aug. 10, 2023).

[2] B. Rizky Rivaldy, “ IMPLEMENTASI GR-GSM UNTUK DECODING KOMUNIKASI GSM TERENKRIPSI,” *e-Proceeding of Applied Science*, vol. Vol.3, pp. 1822-Page 1832, 2017.

[3] R. Efriyendro and Y. Rahayu, “Analisa Perbandingan Kuat Sinyal 4G LTE antara Operator Telkomsel dan XL AXIATA Berdasarkan Paramater Drive Test Menggunakan Software G-NetTrack Pro di Area Jalan Protokol Panam.,” *Jurnal Online Mahasiswa Fakultas Teknik Universitas Riau*, vol. 4, pp. 1–9, Sep. 2017.

[4] G. Heine, *GSM Networks: Protocols, Terminology, and Implementation*. Boston : Artech House mobile communications library, 1998.

[5] D. S. M. Gultom and Widjaja. Damar, “SISTEM PEMANTAUAN IDENTITAS JARINGAN GSM,” *Seminar Nasional Aplikasi Teknologi Informasi* , pp. G26–G31, 2009.