Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia p-ISSN 2086-5805
Akademi Angkatan Udara | Yogyakarta, 27 November 2023 e-ISSN 2808-2540
Volume 5, Tahun 2023, hlm. 277-290 10.54706/senastindo.v7.2025.40 

# Pengembangan *Mobile-IMSI Catcher* Berbasis OsmocomBB dan Pesawat Tanpa Awal

## *Development of Mobile-IMSI Cacther Based on OsmocomBB and Unmanned Aerial Vehicle*

**Dedy Hariyadi[1*], Fazlurrahman[2], Mei Purweni[3]**

[1] Universitas Jenderal Achmad Yani Yogyakarta
*E-mail: dedy@unjaya.ac.id*
[2] Komunitas NgeSec Yogyakarta
*E-mail: fazlurbima@gmail.com*
[3] Universitas Duta Bangsa Surakarta
*E-mail: meipurweni@gmail.com*

Abstract— ***Penelitian ini bertujuan untuk mengembangkan sistem Mobile-IMSI Catcher yang portabel dan tersembunyi dengan mengintegrasikan perangkat lunak sumber terbuka OsmocomBB dan platform udara Unmanned Aerial Vehicle (UAV). Sistem ini dirancang untuk mendeteksi dan memetakan subscriber identity dari perangkat seluler yang aktif di jaringan GSM, baik dari operator domestik maupun asing, termasuk perangkat yang berada dalam kondisi roaming. Pendekatan yang digunakan dalam penelitian ini menggabungkan konsep Signal Intelligence (SigInt) dan metode Network Penetration Testing berdasarkan kerangka kerja NIST SP 800-42. Tahapan implementasi mencakup pencarian kanal frekuensi Absolute Radio Frequency Channel Number (ARFCN), pemindaian IMSI, serta pengumpulan dan analisis parameter jaringan seperti MCC, MNC, LAC, dan CI. Pengujian dilakukan di wilayah Yogyakarta dengan UAV yang telah dilengkapi sistem OsmocomBB dan modul SDR. Hasilnya menunjukkan bahwa sistem mampu menangkap berbagai subscriber identity, memetakan lokasi perangkat berdasarkan parameter jaringan, dan melacak perpindahan perangkat melalui perubahan LAC dan CI. Visualisasi data disajikan dalam bentuk peta spasial yang mendukung analisis mobilitas perangkat. Integrasi UAV meningkatkan jangkauan dan fleksibilitas sistem, memungkinkan operasi dilakukan secara mobile, stealth, dan efisien. Dengan biaya implementasi yang relatif rendah dan kemampuan operasi udara, sistem ini berpotensi diterapkan dalam skenario pemantauan jaringan seluler, keamanan nasional, penegakan hukum, serta pengembangan sistem intelijen sinyal di masa depan.***

Keywords— **IMSI Catcher, subscriber identity, OsmocomBB, UAV, signal intelligence**

Abstrak— ***This research aims to develop a portable and stealthy Mobile-IMSI Catcher system by integrating the open-source software OsmocomBB with an aerial platform based on an Unmanned Aerial Vehicle (UAV). The system is designed to detect and map subscriber identities from active mobile devices operating on GSM networks, including those from domestic and foreign operators as well as roaming devices. The methodology combines Signal Intelligence (SigInt) principles with the Network Penetration Testing framework based on NIST SP 800-42. The implementation stages include scanning for Absolute Radio Frequency Channel Numbers (ARFCN), capturing IMSI, and collecting and analyzing network parameters such as MCC, MNC, LAC, and CI. Field testing was conducted in the Yogyakarta region using a UAV equipped with OsmocomBB firmware and a Software Defined Radio (SDR) module. The results show that the system successfully captured various subscriber identities, mapped device locations based on network parameters, and tracked movement through changes in LAC and CI values. The collected data were visualized through spatial mapping, enabling detailed mobility analysis. The UAV integration significantly enhances the system's range, operational flexibility, and stealth, allowing data interception to be conducted from the air with minimal risk of detection. With its***

* *Dedy Hariyadi*
*Email: dedy@unjaya.ac.id*

p-ISSN 2685-8991
e-ISSN 2808-2540

***relatively low deployment cost and airborne mobility, this system presents a promising solution for future applications in cellular network monitoring, national security, law enforcement, and signal intelligence operations.***

Kata Kunci— **IMSI Catcher, subscriber identity, OsmocomBB, UAV, signal intelligence**

## I. PENDAHULUAN

IMSI Catcher merupakan perangkat penyadap seluler yang berfungsi sebagai *base station* palsu atau *fake BTS* untuk memperoleh identitas unik pelanggan, yaitu *International Mobile Subscriber Identity* (IMSI) yang tertanam pada kartu SIM. Perangkat ini bekerja dengan menyaru sinyal BTS resmi sehingga mampu mengelabui perangkat pengguna supaya melakukan proses registrasi dan mengungkapkan identitas permanen seperti IMSI maupun *International Mobile Equipment Identity* (IMEI). Informasi ini dapat digunakan untuk tujuan yang beragam, mulai dari pelacakan lokasi, pemantauan komunikasi, hingga penyadapan data seluler [1], [2].

Berbagai penelitian telah mengkaji metode dan pengembangan *IMSI Catcher*. Studi LTRACK, memperkenalkan teknik pelacakan berbasis *sniffing pasif* dan *overshadowing* untuk meningkatkan sifat tersembunyi serangan di jaringan LTE [3]. Sementara itu, FlashCatch difokuskan pada percepatan akuisisi IMSI dengan meminimalkan gangguan layanan yang dialami pengguna [4]. Di sisi lain, eksperimen praktis berbasis *software-defined radio* (SDR) dan perangkat lunak sumber terbuka seperti OpenBTS dan OsmocomBB juga telah menunjukkan bahwa implementasi IMSI Catcher dapat dilakukan dengan biaya rendah dan infrastruktur terbatas [5].

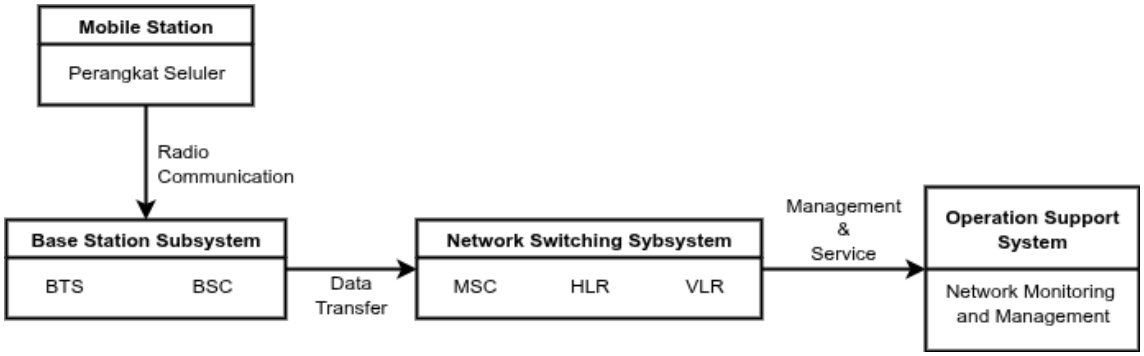
Meskipun demikian, sebagian besar penelitian sebelumnya masih menghadapi keterbatasan yang cukup signifikan. Implementasi IMSI Catcher umumnya berbasis stasiun tetap atau perangkat portabel yang bergantung pada komputer, sehingga mobilitas dan jangkauan operasinya terbatas [6]. Penelitian tentang pemanfaatan OsmocomBB sebagai proyek open source yang masih jarang dilakukan walaupun proyek ini memiliki potensi besar karena menyediakan akses langsung pada baseband GSM, DECT, TETRA, dan lain-lain [7]. Hingga saat ini, belum ditemukan penelitian komprehensif yang secara eksplisit mengintegrasikan OsmocomBB dan UAV untuk membangun sistem IMSI Catcher berbasis udara. Padahal, kombinasi ini berpotensi signifikan dalam meningkatkan mobilitas, jangkauan, dan sifat stealth dari operasi penyadapan seluler. Potensi ini membuka peluang penelitian IMSI Catcher yang saat ini masih berfokus pada pengembangan berbasis darat, tanpa mempertimbangkan potensi UAV sebagai platform operasi seluler bergerak [8].

Berdasarkan permasalahan tersebut, penelitian ini mengusulkan pengembangan *IMSI Catcher* berbasis OsmocomBB yang terintegrasi dengan UAV. Pendekatan ini diharapkan dapat mengatasi keterbatasan mobilitas dan jangkauan pada penelitian sebelumnya, sekaligus meningkatkan efisiensi serta sifat tersembunyi operasi *IMSI Catcher*. Dengan memanfaatkan fleksibilitas OsmocomBB sebagai pengendali baseband GSM dan UAV sebagai platform udara, penelitian ini bertujuan menghasilkan perangkat *IMSI Catcher* yang portabel, efisien, sulit terdeteksi, serta relevan untuk skenario keamanan jaringan seluler masa depan.

# II. LANDASAN TEORI

## A. *Jaringan GSM dan Subcriber Identity*

*Global System for Mobile Communications* (GSM) merupakan standar komunikasi seluler digital yang memiliki struktur modular, terdiri dari *Mobile Station* (MS), *Base Station Subsystem* (BSS), *Network Switching Subsystem* (NSS), dan *Operation Support System* (OSS). MS mencakup perangkat dan kartu SIM yang menyimpan *subscriber identity* atau identitas pelanggan. BSS terdiri atas *Base Transceiver Stations* (BTS) dan *Base Station Controllers* (BSC) yang menangani komunikasi radio dan manajemen kanal, sedangkan NSS mengelola pemrosesan panggilan dan pelacakan pelanggan melalui *Mobile Switching Center* (MSC), *Home Location Register* (HLR), dan *Visitor Location Register* (VLR). OSS mendukung pengawasan serta pemeliharaan jaringan, menjadikan keseluruhan arsitektur GSM cukup andal dan skalabel dalam penyediaan layanan komunikasi dasar seperti terlihat pada Gambar 1. Berikut.




Gambar 1. Aristektur GSM

Meskipun arsitektur GSM dirancang secara modular dan terstandarisasi, sistem ini memiliki kelemahan fundamental dalam aspek keamanan identitas pelanggan. International Mobile Subscriber Identity (IMSI) yang berfungsi sebagai identitas permanen pengguna dikirim dalam bentuk plaintext pada saat registrasi awal ke jaringan. Proses ini dapat dieksploitasi oleh perangkat IMSI Catcher yang beroperasi sebagai Base Transceiver Station (BTS) palsu untuk memperoleh IMSI secara ilegal. Ketidaktersediaan mekanisme autentikasi dua arah antara perangkat dan BTS menyebabkan perangkat pengguna selalu menerima koneksi dari BTS yang mengklaim sebagai bagian dari jaringan resmi. Kondisi tersebut menghasilkan kerentanan sistemik terhadap penyadapan dan pelacakan lokasi yang bersifat tidak sah [10].

## B. *IMSI Catchers*

*IMSI Catcher* merupakan perangkat penyadapan yang beroperasi sebagai BTS palsu untuk memaksa perangkat seluler melakukan koneksi dan mengirimkan IMSI. Perangkat ini memanfaatkan kelemahan dalam protokol autentikasi jaringan seluler, khususnya pada sistem GSM dan LTE yang tidak menerapkan autentikasi dua arah antara perangkat dan BTS. Ketika BTS palsu memancarkan sinyal dengan intensitas lebih tinggi daripada BTS resmi, perangkat seluler secara otomatis melakukan koneksi dan mengirimkan IMSI tanpa validasi terhadap legitimasi sumber sinyal [11].

Hasil penelitian eksperimental menunjukkan bahwa *IMSI Catcher* dapat dibangun dengan memanfaatkan perangkat lunak berlisensi bebas dan perangkat keras berbiaya rendah. Konfigurasi ini menghasilkan perangkat yang portabel dan mudah direplikasi untuk berbagai skenario operasional. Penggunaan IMSI Catcher tidak terbatas pada jaringan 2G, tetapi juga berhasil mengeksploitasi kerentanan pada perangkat yang terhubung ke jaringan 4G dan 5G. Penerapan sistem enkripsi dan autentikasi pada jaringan generasi baru belum sepenuhnya mengeliminasi celah keamanan, khususnya pada mekanisme fallback ke jaringan legacy yang

p-ISSN 2685-8991
e-ISSN 2808-2540

masih digunakan oleh sebagian besar perangkat. Berdasarkan temuan tersebut, *IMSI Catcher* merupakan ancaman yang terverifikasi secara empiris terhadap keamanan jaringan dan perlindungan identitas pelanggan dalam sistem komunikasi seluler modern [12].

### *C. Software Defined Radio dan OsmocomBB*

*Software Defined Radio* (SDR) merupakan teknologi komunikasi radio yang mengalihkan fungsi perangkat keras konvensional ke dalam bentuk perangkat lunak. Seluruh proses pengolahan sinyal seperti modulasi, demodulasi, dan filtrasi dilakukan melalui pemrograman digital. Teknologi ini menghasilkan sistem komunikasi yang fleksibel dan dapat disesuaikan secara langsung untuk mendukung berbagai protokol jaringan. Berdasarkan studi eksperimental, SDR seperti USRP B210 telah digunakan secara efektif dalam pengujian dan validasi transmisi sinyal LTE dalam mode MIMO. SDR terbukti mampu menangani komunikasi multi-antena serta mendukung analisis spektrum secara *real-time* pada jaringan seluler generasi terbaru [13].

OsmocomBB merupakan perangkat lunak berlisensi bebas yang menyediakan akses penuh terhadap fungsi *baseband* dalam sistem GSM. Platform ini digunakan dalam penelitian jaringan seluler untuk membangun BTS palsu, melakukan pemantauan sinyal, dan merekonstruksi proses autentikasi perangkat. Integrasi OsmocomBB dengan modul SDR menghasilkan perangkat *transceiver* yang mampu menjalankan fungsi *IMSI Catcher* secara presisi dan efisien. Berdasarkan studi terbaru, OsmocomBB telah berhasil digunakan dalam eksperimen penyadapan komunikasi GSM dan analisis lalu lintas jaringan lapisan rendah dengan akurasi yang dapat diverifikasi secara teknis [14].

### *D. Unmanned Aerial Vehicle (UAV) for Mobile Interception*

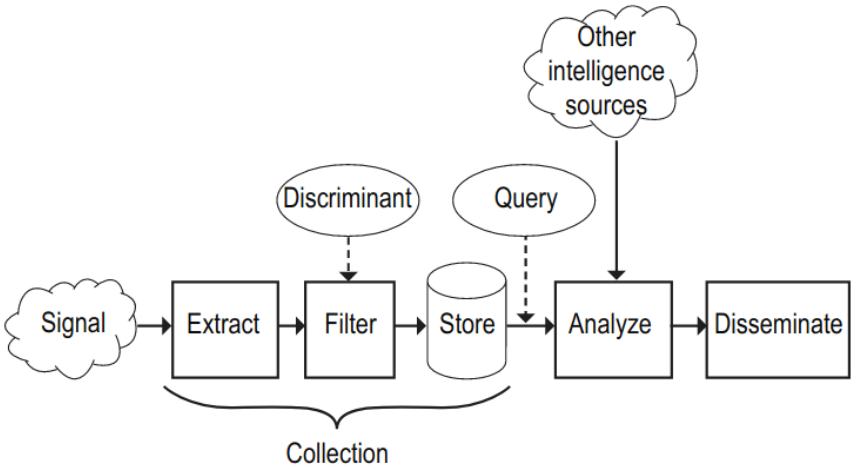
*Unmanned Aerial Vehicle* (UAV) telah berkembang menjadi platform yang digunakan secara luas dalam bidang komunikasi nirkabel. Integrasi UAV dengan jaringan seluler memberikan fleksibilitas operasional yang tinggi karena dapat beroperasi pada ketinggian tertentu untuk memperluas cakupan sinyal, meningkatkan kualitas layanan, dan menjangkau wilayah yang sulit diakses. Penelitian sebelumnya bahwa UAV dapat digunakan sebagai *mobile base station* berbasis LTE dan 5G, khususnya dalam skenario darurat, pemantauan, dan penegakan hukum [15]. Peran UAV sebagai *node* jaringan udara memungkinkan peningkatan jangkauan layanan serta mendukung keberlangsungan komunikasi pada daerah yang infrastruktur komunikasinya terbatas.

Selain mendukung layanan komunikasi, UAV berpotensi digunakan untuk operasi khusus berbasis *interception*. Penelitian eksperimental menunjukkan bahwa UAV yang dilengkapi modul GSM base station mampu melakukan lokalisasi perangkat seluler target dengan memanfaatkan deteksi arah sinyal [16]. Sistem ini telah berhasil digunakan dalam operasi pencarian dan penyelamatan dengan memaksa perangkat seluler target masuk ke *mode* darurat untuk kemudian terhubung ke BTS yang dipasang pada UAV. Berbeda dengan penelitian sebelumnya yang umumnya mengimplementasikan *IMSI Catcher* dalam bentuk perangkat portabel berbasis darat, penelitian ini mengusulkan pendekatan udara berbasis UAV untuk meningkatkan mobilitas, jangkauan, dan efektivitas identifikasi pelanggan. Kontribusi utama dari penelitian ini adalah pembangunan IMSI Catcher mobile berbasis OsmocomBB yang terintegrasi dengan UAV, sebagai solusi interception bersifat stealth dengan jangkauan luas dan biaya rendah.

## III. METODE PENELITIAN

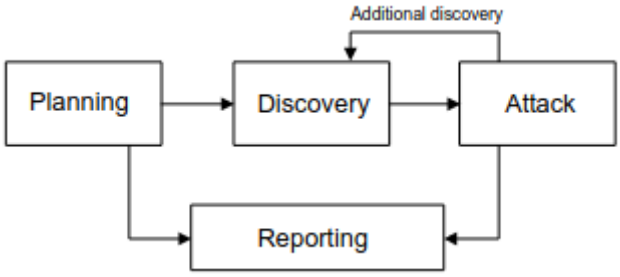
*Signal Intelligence* (SigInt) menjadi dasar dalam penelitian ini, secara umum definisikan sebagai bidang keilmuan intelijen yang berfokus pada pengumpulan, pemantauan, dan analisis sinyal elektromagnetik untuk menghasilkan informasi strategis maupun taktis [17]. Berdasarkan konsep dasar yang diusulkan oleh *National Academies of Sciences* terdapat 5 tahapan utama

seperti 281. SigInt dimulai dari tahap ekstraksi (*extract*), yaitu pengumpulan dan ekstraksi sinyal mentah dari berbagai sumber dalam penelitian ini berdasarkan *IMSI Cacther*. Data yang diperoleh kemudian melalui tahap penyaringan (*filter*) untuk membatasi informasi hanya pada target tertentu dengan parameter yang telah ditentukan. Informasi hasil penyaringan selanjutnya masuk ke tahap penyimpanan (*store*), yaitu penyimpanan data sebagai arsip resmi yang siap dianalisis. Proses analisis (analyze) dilakukan oleh analis melalui query data dan integrasi dengan sumber intelijen lainnya guna menghasilkan pengetahuan yang komprehensif. Tahap akhir adalah diseminasi (*disseminate*), yaitu penyebaran produk intelijen kepada pihak berwenang atau pembuat kebijakan [18]. Berikut metode *Signal Intelligence seperti yang ditnjukkan pada Gambar 2.*




Gambar 2. Metode *Signal Intelligence* [18]

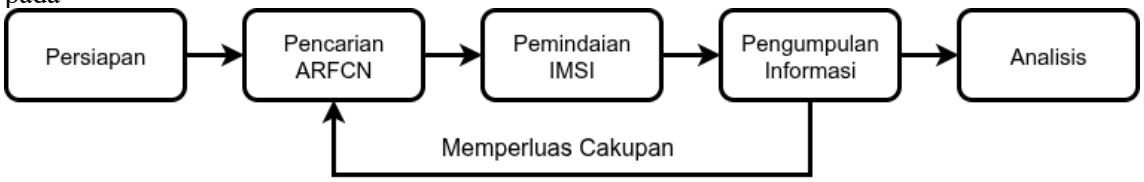
Konsep dasar SigInt dipadukan dengan metode penetration testing berdasarkan NIST SP 800-42 yang terdiri dari 4 tahapan, yaitu yaitu *Planning, Discovery, Attack*, dan *Reporting* seperti pada 281. Tahap *Planning* menekankan penyusunan ruang lingkup, aturan pelaksanaan, dan persetujuan formal dari manajemen untuk memastikan pengujian berjalan terkendali. Tahap *Discovery* meliputi aktivitas pengumpulan informasi awal seperti *network scanning*, analisis kerentanan, dan enumerasi target guna mengidentifikasi celah keamanan yang tersedia. Tahap *Attack* merupakan proses verifikasi kerentanan dengan melakukan eksploitasi langsung menggunakan teknik serangan yang umumnya digunakan penyerang nyata, sehingga dapat menilai tingkat risiko dan potensi dampak yang ditimbulkan. Tahap terakhir, *Reporting*, menghasilkan dokumentasi formal yang merangkum kerentanan yang ditemukan, tingkat keparahan, serta rekomendasi teknis untuk mitigasi. Proses ini juga bersifat iteratif, di mana hasil dari tahap *Attack* dapat kembali memicu tahap *Discovery* tambahan untuk mengidentifikasi celah yang lebih dalam [19].



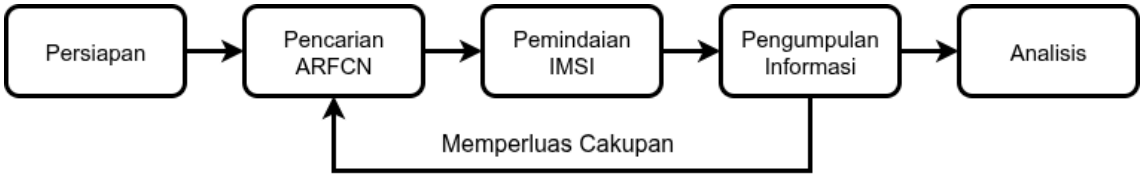

Gambar 3. Metode Network Penetration Testing [19]

p-ISSN 2685-8991
e-ISSN 2808-2540

Kedua metode SigInt dan *Network Penetration Testing* diadaptasi pada implementasi *Mobile-IMSI Catcher* menjadi beberapa tahapan, yaitu Persiapan, Pencarian *Absolute Radio Frequency Channel Number* (ARFCN), Pemindaian IMSI, Pengumpulan Informasi, dan Analisis seperti pada




Gambar 4. Tahapan penelitian dimulai dari Persiapan (Planning), yaitu penetapan ruang lingkup, konfigurasi perangkat keras dan perangkat lunak, dan parameter teknis yang digunakan. Proses dilanjutkan dengan Pencarian ARFCN (*Discovery*) untuk menentukan kanal frekuensi uplink dan downlink yang aktif pada BTS sekitar yang menjadi dasar bagi tahap Pemindaian IMSI (*Discovery*) untuk mendeteksi subcriber identity yang terkoneksi pada kanal tersebut. Data hasil pemindaian dicatat pada tahap Pengumpulan Informasi (*Collection*) yang mencakup pencatatan IMSI, TMSI, MCC, MNC, LAC, dan CI berdasarkan ARFCN yang digunakan. Tahap terakhir adalah Analisis (*Analyze*), yaitu pengolahan data yang difokuskan pada prediksi lokasi perangkat seluler yang teridentifikasi dengan visualisasi berupa peta. Seluruh proses bersifat iteratif karena keluaran dari tahap Pengumpulan Informasi dapat kembali ke aktivitas Pencarian ARFCN untuk memperluas cakupan subcriber identity dan meningkatkan akurasi penentuan lokasi. Mekanisme ini sejalan dengan peneltian sebelumnya yang menunjukkan bahwa *IMSI Catcher* memanfaatkan karakteristik pesan identitas yang terekspos dalam lalu lintas seluler dan serta pemilihan kanal frekuensi sebagai faktor kunci dalam proses *subcriber identification* [20].



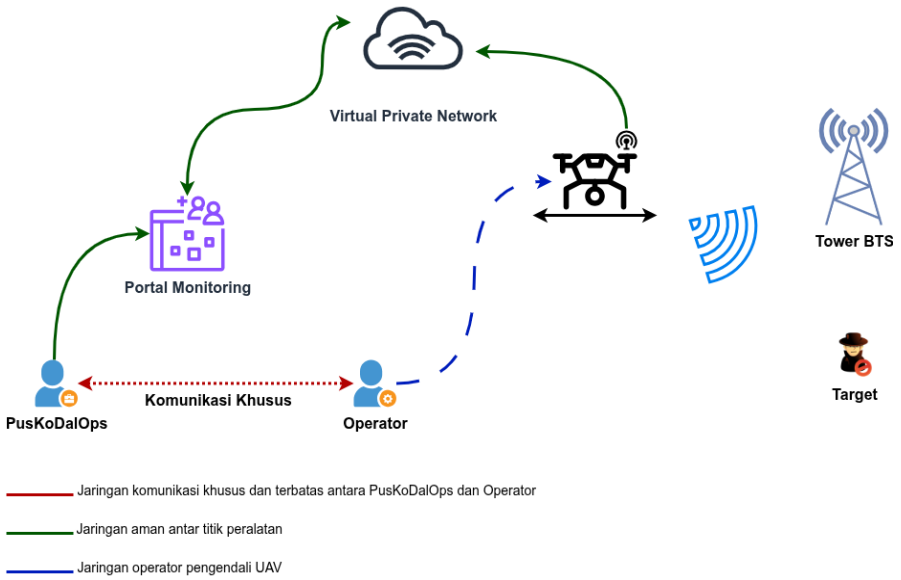

Gambar 4. Implementasi *Mobile-IMSI Catcher*

## IV. HASIL DAN PEMBAHASAN

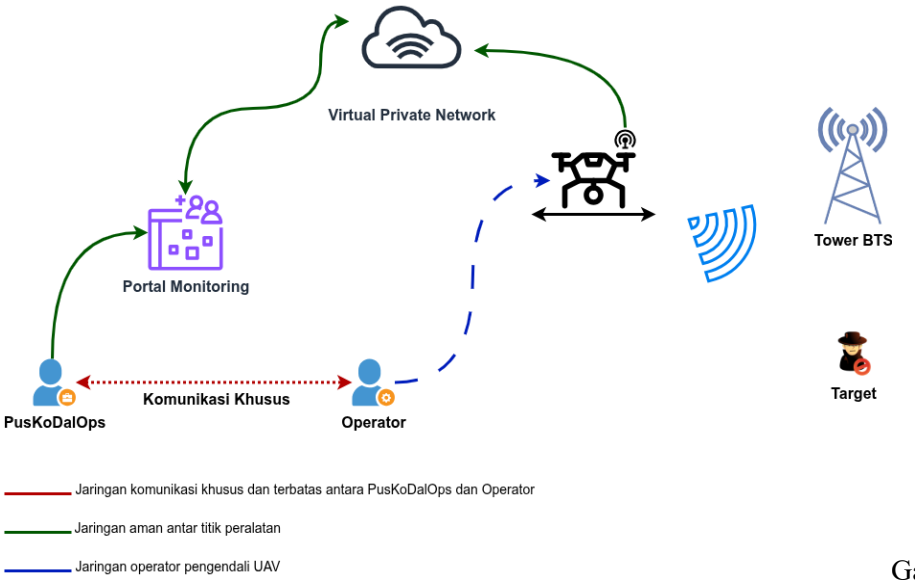
### *A. Persiapan dan Perencanaan*

*Mobile-IMSI Catcher* dirancang menggunakan komunikasi khusus, terjaga, dan terbatas antara portal monitoring dan proses pengumpulan informasi. Ketua Tim pada Pusat Komando dan Pengendalian Operasi melakukan komunikasi dengan Operator di lapangan melalui jaringan khusus. Standar operasional prosedur disampaikan oleh Ketua Tim sebagai bagian dari tahap Perencanaan operasi menggunakan *Mobile-IMSI Catcher*. Persiapan UAV dilakukan oleh Operator, dengan memastikan bahwa firmware OsmocomBB telah terinstal dan berfungsi dengan baik berdasarkan koordinasi antara Ketua Tim dan Operator. Adapun alur pengoperasian *Mobile-*

*IMSI* *Catcher* seperti pada




Gambar 5. Alur *Mobile-IMSI Catcher*




Gambar 5.

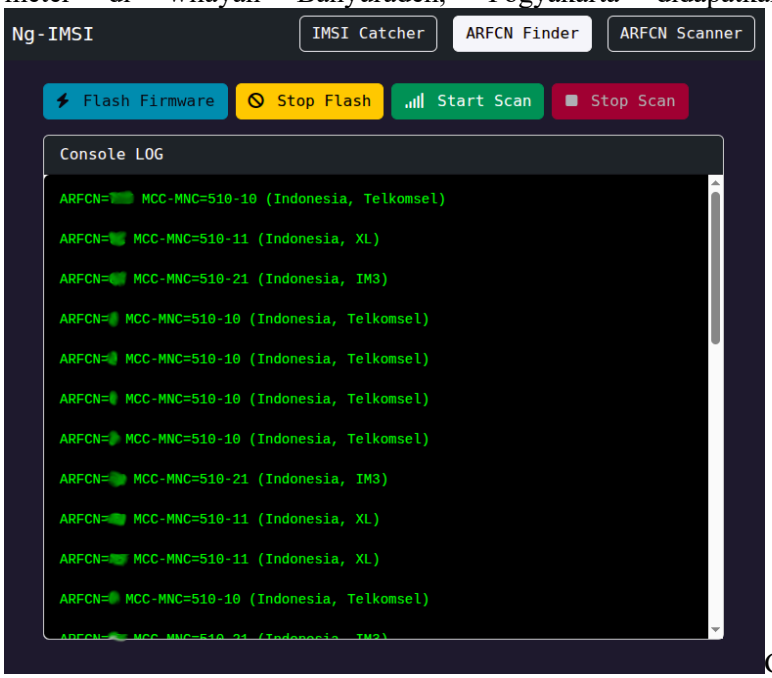
## *B. Pencarian ARFCN*

*Absolute Radio Frequency Channel Number* (ARFCN) adalah nomor kanal unik dalam GSM yang mengidentifikasi pasangan frekuensi *uplink* dan *downlink* pada BTS. Penomoran ini mencegah interferensi antar sel dengan pita frekuensi pemisah sebesar 45 MHz dan memastikan perangkat seluler melakukan registrasi pada kanal yang sesuai. Dalam konteks keamanan,

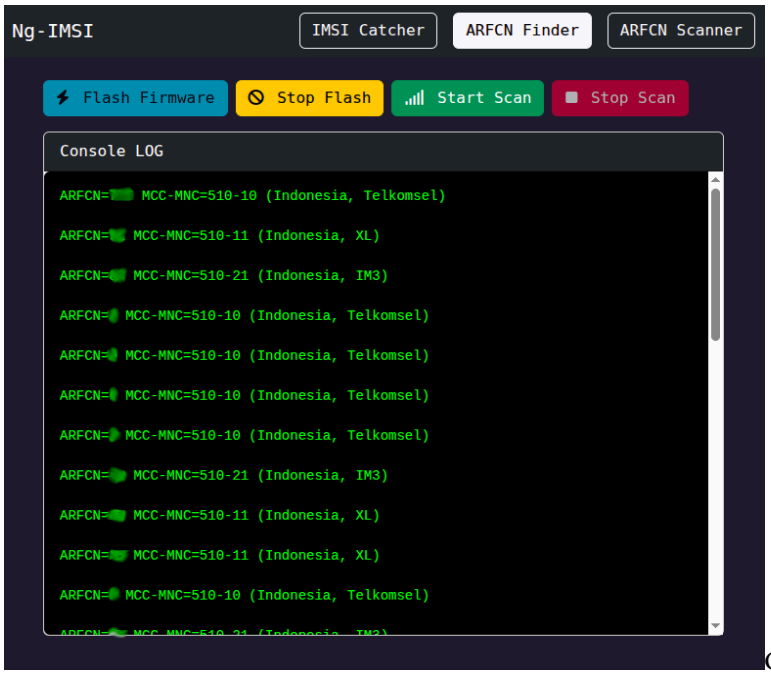
p-ISSN 2685-8991
e-ISSN 2808-2540

ARFCN dapat dieksploitasi untuk membangun BTS palsu (*fake cell)* yang memaksa perangkat terkoneksi, sehingga *IMSI Catcher* berhasil mengungkap *subcriber identity* [21].

Setelah tahap instalasi *firmware* OsmocomBB, tahapan selanjutnya adalah menerbangkan UAV sesuai perkiraan lokasi target dengan menjalankan tahapan Pencarian ARFCN (*ARFCN Finder*). Setiap operator telekomunikasi telah memiliki penomoran kanal sesuai dengan regulasi masing-masing negara. Berdasarkan Pencarian ARFCN menggunakan UAV pada ketinggian sekitar 30 meter di wilayah Banyuraden, Yogyakarta didapatkan daftar ARFCN seperti




Gambar 6. Sedangkan persentase dari hasi Pencarian ARFCN tampak seperti pada TABEL 1.




Gambar 6. Pencarian ARFCN

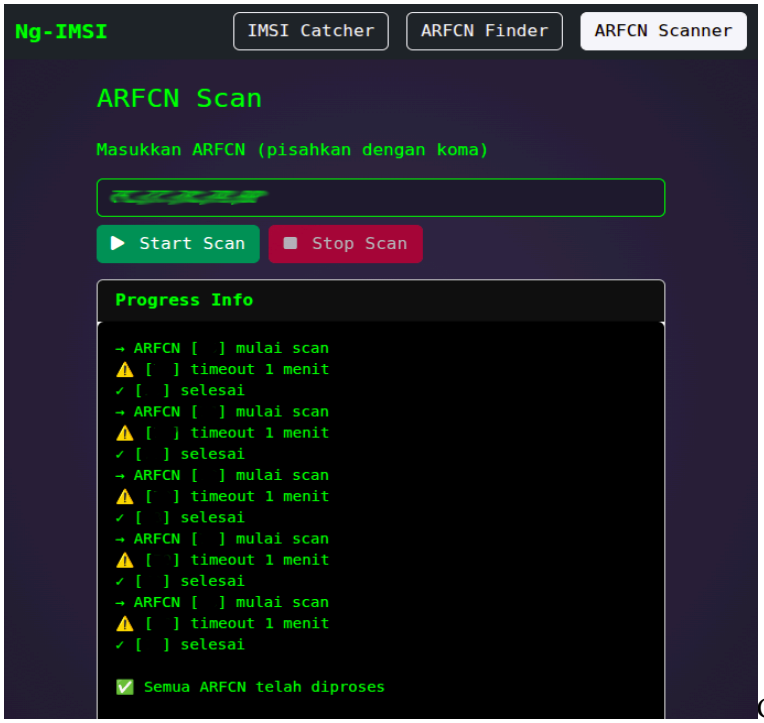
TABEL 1
HASIL PENCARIAN ARFCN

| Operator | Kategori Band | Persensate |
|---|---|---|
| IM3 | GSM 1800 | 53.33% |
| IM3 | GSM 900 | 46.67% |
| Telkomsel | GSM 1800 | 62.50% |
| Telkomsel | GSM 900 | 37.50% |
| XL | GSM 1800 | 50.00% |
| XL | GSM 900 | 50.00% |

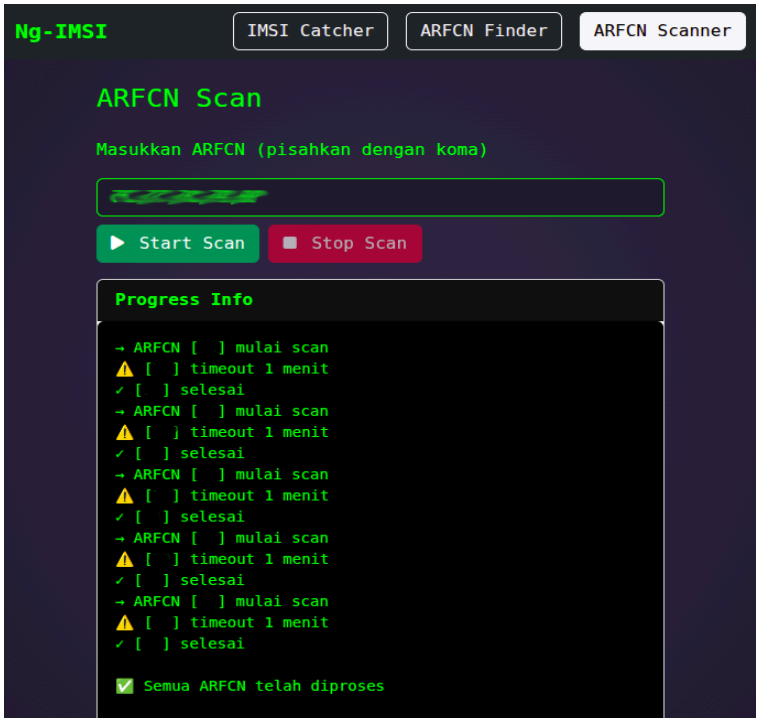
## *C. Pemindaian IMSI*

Daftar ARFCN yang diperoleh pada tahapan Pencarian ARFCN berfungsi sebagai tolok ukur untuk mengidentifikasi kanal frekuensi yang digunakan oleh BTS dalam proses komunikasi seluler melalui tahapan Pemindaian IMSI, seperti pada

p-ISSN 2685-8991
e-ISSN 2808-2540




Gambar 7. Informasi ini penting karena setiap ARFCN merepresentasikan jalur *uplink* dan *downlink* tertentu yang menghubungkan perangkat pengguna dengan jaringan. Dengan mendasarkan pengamatan pada ARFCN, proses pencatatan komunikasi difokuskan pada kanal yang relevan sehingga menghasilkan pengungkapan *subscriber identity*. Pada tahap berikutnya, *Mobile-IMSI Catcher* memanfaatkan kanal tersebut untuk memaksa perangkat melakukan registrasi ulang yang kemudian menampilkan International IMSI sebagai identitas permanen pelanggan.




Gambar 7. Pemindaian IMSI

*D. Pengumpulan Informasi*


Hasil pemindaian IMSI pada Gambar 8 menunjukkan bahwa perangkat IMSI Catcher berhasil memperoleh identitas pelanggan dari berbagai operator, baik nasional maupun asing, yang sedang terhubung ke jaringan seluler. Data yang terekam menampilkan IMSI sebagai identitas permanen pelanggan dan TMSI sebagai identitas sementara, disertai dengan parameter jaringan berupa MCC (*Mobile Country Code*), MNC (*Mobile Network Code*), LAC (*Location Area Code*), dan CI (*Cell Identi*ty). Analisis distribusi MCC–MNC memperlihatkan bahwa sebagian besar IMSI yang diperoleh berasal dari MCC 510 (Indonesia), dengan kode MNC 1, 10, 11, dan 897. Selain itu, terdapat pula IMSI dari MCC 525 (Singapura), MCC 460 (Tiongkok) dan MCC 310 (Amerika Serikat) yang menunjukkan adanya pengguna dalam kondisi *roaming*. *Mobile-IMSI Catcher* tidak hanya efektif dalam mengungkap identitas pelanggan domestik, tetapi juga mampu mendeteksi pelanggan asing yang sedang terhubung ke jaringan lokal. Dengan adanya parameter LAC dan CI yang menyertai setiap IMSI, data yang diperoleh berpotensi untuk pemetaan lokasi pelanggan dan visualisasi

p-ISSN 2685-8991
e-ISSN 2808-2540


Gambar 8. Pengumpulan Informasi IMSI

spasial dalam bentuk peta, sehingga memperluas cakupan analisis dari sekadar identifikasi pelanggan menuju aspek geolokasi jaringan.

### *E. Analisis dan Pemetaan*

Berdasarkan tahapan Pengumpulan Informasi IMSI, luaran yang diperoleh berupa tiga komponen utama, yaitu catatan lengkap seluruh subscriber identity dalam bentuk berkas CSV, subscriber identity tanpa duplikasi IMSI dalam bentuk berkas CSV, dan visualisasi pemetaan. Catatan lengkap seluruh subscriber identity digunakan untuk menganalisis pergerakan perangkat seluler melalui perubahan *Location Area Code* (LAC) dan *Cell Identity* (CI). Sedangkan berkas subscriber identity tanpa duplikasi IMSI dimanfaatkan untuk mempermudah analisis jumlah pelanggan unik yang terhubung dengan BTS.

Catatan lengkap seluruh subscriber identity dapat mengidentifikasi mobilitas suatu perangkat, seperti pada TABEL 2. Perangkat dengan IMSI 460********** terekam melalui perubahan parameter jaringan dalam rentang waktu 12:09:08 hingga 12:17:11, ditunjukkan oleh perubahan parameter jaringan dari LAC 4787/CI 42666 ke LAC 4767/CI 51448. Perubahan LAC dan CI tersebut merepresentasikan perpindahan antar sel BTS yang memicu prosedur *location update*, sehingga proses registrasi ulang perangkat pada jaringan menghasilkan rekaman identitas pelanggan selama pemindaian IMSI.

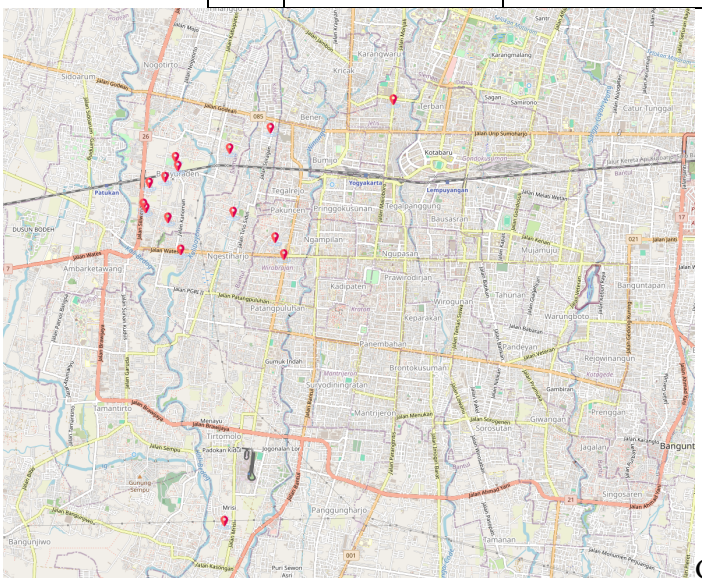
TABEL 2
CONTOH CATATAN SELURUH SUBCRIBER IDENTITY

| IMSI | MNC | MCC | LAC | IC | Waktu |
|---|---|---|---|---|---|
| 460********** | 460 | 91 | 4767 | 51448 | 12:17:11 |
| 460********** | 460 | 91 | 4787 | 42666 | 12:09:08 |

Luaran berupa *subscriber identity* tanpa duplikasi IMSI digunakan untuk mengidentifikasi perangkat asing yang terhubung ke jaringan seluler lokal. Data ini juga dimanfaatkan untuk menghitung jumlah pelanggan unik berdasarkan operator, sehingga dapat menggambarkan distribusi koneksi antar operator secara lebih akurat. Dengan demikian, luaran tersebut berperan penting dalam analisis jumlah dan karakteristik pelanggan yang berhasil ditangkap oleh *IMSI Catcher*. Berdasarkan TABEL 3 terlihat bahwa mayoritas pelanggan yang terdeteksi berasal dari operator lokal, dengan dominasi Telkomsel sebanyak 54.55% dari total data yang dikumpulkan.

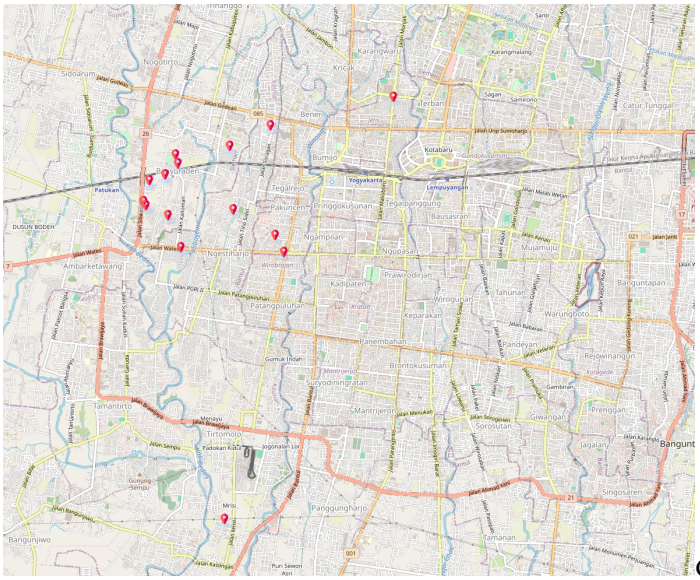
TABEL 3
ANALISIS OPERATOR SELULER

| No | Negara | Operator | Jumlah |
|---|---|---|---|
| 1 | Amerika Serikat | T-Mobile | 1.40% |
| 2 | China | China Unicom | 4.90% |
| 3 | China | China Telecom | 0.70% |
| 4 | Singapura | SingTel | 0.70% |
| 5 | Indonesia | Telkomsel | 54.55% |
| 6 | Indonesia | XL | 30.77% |
| 7 | Indonesia | Indosat | 4.20% |
| 8 | Indonesia | Smartfren | 2.80% |



Gambar 9 merupakan hasil pemetaan menggunakan *mobile-IMSI Catcher* menunjukkan bahwa identitas pelanggan seluler berhasil ditangkap pada berbagai lokasi. Pola distribusi ini menegaskan kemampuan *mobile-IMSI Catcher* tidak hanya dalam memperoleh identitas pelanggan, tetapi juga dalam memetakan distribusi pengguna seluler dan pergerakan perangkat berdasarkan lokasi geografis, sehingga dapat digunakan untuk analisis mobilitas dan pemantauan jaringan secara lebih komprehensif.

p-ISSN 2685-8991
e-ISSN 2808-2540



Gambar 9. Visualisasi Pemetaan Hasil *Mobile-IMSI Catcher*

## V. KESIMPULAN

Penelitian ini berhasil mengembangkan sistem *Mobile-IMSI Catcher* berbasis OsmocomBB yang terintegrasi dengan UAV untuk mendeteksi dan memetakan *subscriber identity* secara *mobile*. Sistem ini mampu mengungkap *subscriber identity* dari berbagai operator, termasuk perangkat asing dalam kondisi roaming, dan memvisualisasikan distribusinya berdasarkan parameter jaringan seperti MCC, MNC, LAC, dan CI. Integrasi UAV memberikan keunggulan dalam mobilitas, jangkauan, dan kemampuan operasi tersembunyi, menjadikan sistem ini efektif digunakan dalam skenario pemantauan jaringan seluler dan intelijen sinyal.

Penelitian selanjutnya disarankan untuk mengoptimalkan perangkat keras agar lebih ringan, hemat daya, dan sesuai untuk integrasi pada UAV miniatur demi meningkatkan mobilitas dan kemampuan *stealth*. Selain itu, pengembangan sistem agar mendukung jaringan 4G dan 5G melalui pemanfaatan celah keamanan pada mekanisme fallback ke jaringan *legacy* akan memperluas cakupan identifikasi *subscriber identity* pada perangkat modern dan memperkuat kontribusi sistem terhadap keamanan jaringan seluler generasi baru.

## REFERENSI

[1] P. Ziayi, S. M. Farmanbar, dan M. Rezvani, "YAICD: Yet Another IMSI Catcher Detector in GSM," *Security and Communication Networks*, vol. 2021, hlm. 1–13, Jan 2021, doi: 10.1155/2021/8847803.

[2] I. Palamà, F. Gringoli, G. Bianchi, dan N. Blefari-Melazzi, "IMSI Catchers in the wild: A real world 4G/5G assessment," *Computer Networks*, vol. 194, hlm. 108137, Jul 2021, doi: 10.1016/j.comnet.2021.108137.

[3] M. Kotuliak, S. Erni, P. Leu, M. Röschlin, dan S. ˇCapkun, "LTRACK: Stealthy Tracking of Mobile Phones in LTE," dalam *Proceedings of the 31st USENIX Security Symposium, Security 2022*, Boston, MA: USENIX Association, 2022. [Daring]. Tersedia pada: https://www.scopus.com/pages/publications/85140951883

[4] A. Paci, G. Bologna, I. Palamà, dan G. Bianchi, "FlashCatch: Minimizing Disruption in IMSI Catcher Operations," dalam *18th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, Arlington VA USA: ACM, Jun 2025, hlm. 124–135. doi: 10.1145/3734477.3734705.

[5] N. Bello dan O. Kanu, "Penetration Testing of GSM Network Using Man-in-the-Middle Attack," *JES. Journal of Engineering Sciences*, vol. 0, no. 0, hlm. 0–0, Okt 2023, doi: 10.21608/jesaun.2023.226718.1249.

[6] S. Park, R. Borgaonkar, A. Shaik, dan J.-P. Seifert, "Anatomy of Commercial IMSI Catchers and Detectors," dalam *Workshop on Privacy in the Electronic Society*, London, 2019, hlm. 74–86.

[7] S. Iqbal dan J. M. Hamamreh, "Wireless Open Source Supremacy: Osmocom-based Networks for Indoor and Outdoor IoT Applications Deployment," *RS Open Journal on Innovative Communication Technologies*, vol. 4, no. 9, Nov 2023, doi: https://doi.org/10.46470/03d8ffbd.d488f834.

[8] Y. Richter, E. Danieli, I. Levi, dan R. Richter, "A Taxonomy of Multi-Modal Cyber Radio Frequency (CRF) Mitigation Based on Passive Geo-Location and Hardware Characteristics," dalam *2024 IEEE International Conference on Microwaves, Communications, Antennas, Biomedical Engineering and Electronic Systems (COMCAS)*, Tel Aviv, Israel: IEEE, Jul 2024, hlm. 1–6. doi: 10.1109/COMCAS58210.2024.10666202.

[9] P. Sukhno dan S. Sotnik, "Critical Review of GSM Network Structure," dalam *Proceedings of VIII st International Conference*, Kharkiv, Okt 2024.

[10] B. I. Bakare dan S. M. Ekolama, "Preventing Man-in-The-Middle (MiTM) Attack of GSM Calls," *EJECE*, vol. 5, no. 4, hlm. 63–68, Agu 2021, doi: 10.24018/ejece.2021.5.4.336.

[11] A. R, S. Ramesh, V. V. Balaji, Y. Sikhwal, dan Prof. B. Reddy, "Stingray Device for Cyber-Surveillance using a Software-Defined Radio as an IMSI Catcher," *IJRASET*, vol. 11, no. 5, hlm. 1806–1813, Mei 2023, doi: 10.22214/ijraset.2023.51956.

[12] K. M. Kareem, "The Impact of IMSI Catcher Deployments on Cellular Network Security: Challenges and Countermeasures in 4G and 5G Networks," 2024, *arXiv*. doi: 10.48550/ARXIV.2405.00793.

[13] N. Sheremet dan G. Fokin, "Software-Defined Radio Wireless Communication Technology Design. LTE MIMO Mode Validation," dalam *2024 Wave Electronics and its Application in Information and Telecommunication Systems (WECONF)*, St. Petersburg, Russian Federation: IEEE, Jun 2024, hlm. 1–6. doi: 10.1109/WECONF61770.2024.10564644.

[14] A. Savochkin, R. Gasparyan, A. Lukyanchikov, E. Redkina, dan A. Nochovnyi, "Review and study of software packages for emulating 2G/4G mobile networks," dalam *Third International Conference on Optics, Computer Applications, and Materials Science (CMSD-III 2023)*, S. Sadullozoda dan R. Abdullozoda, Ed., Dushanbe, Tajikistan: SPIE, Feb 2024, hlm. 48. doi: 10.1117/12.3025072.

[15] W. Saad, M. Bennis, M. Mozaffari, dan X. Lin, *Wireless Communications and Networking for Unmanned Aerial Vehicles*, 1 ed. Cambridge University Press, 2020. doi: 10.1017/9781108691017.

[16] C. Dorn, A. Depold, F. Lurz, S. Erhardt, dan A. Hagelauer, "UAV-based Localization of Mobile Phones for Search and Rescue Applications," dalam *2022 IEEE 22nd Annual Wireless and Microwave Technology Conference (WAMICON)*, Clearwater, FL, USA: IEEE, Apr 2022, hlm. 1–4. doi: 10.1109/WAMICON53991.2022.9786189.

10, no. 3, hlm. 1–8, Des 2024, doi: 10.33130/AJCT.2024v10i03.005.

[18] Computer Science and Telecommunications Board, *Bulk Collection of Signals Intelligence: Technical Options*. Washington, D.C.: National Academies Press, 2015, hlm. 19414. doi: 10.17226/19414.

[19] K. Scarfone, M. Souppaya, A. Cody, dan A. Orebaugh, "NIST SP 800-42: Guideline on Network Security