# ABSTRAK

**ANALISIS KEAMANAN 5G *STANDALONE* TERHADAP SERANGAN *MAN-IN-THE-MIDDLE* DENGAN EKSPLOITASI DESINKRONISASI *SEQUENCE NUMBER***
**(2026 : XV + 93 Halaman + 20 Gambar + 9 Tabel + 13 Lampiran)**

---

**AN NISA**
**062240352280**
**JURUSAN TEKNIK ELEKTRO**
**PROGRAM STUDI SARJANA TERAPAN TEKNIK TELEKOMUNIKASI**
**POLITEKNIK NEGERI SRIWIJAYA**

Arsitektur jaringan 5G Standalone membawa peningkatan performa komunikasi, namun prosedur otentikasinya masih rentan terhadap ancaman penyadapan. Penelitian ini mengevaluasi kerentanan sistem terhadap serangan Man-in-the-Middle dan metode mitigasi komprehensif untuk menangani masalah keamanan tersebut. Mengandalkan Open5GS sebagai jaringan inti dan UERANSIM sebagai simulator stasiun pemancar dan perangkat pengguna, pengujian dilakukan dalam lingkungan tervirtualisasi. Metode yang digunakan termasuk manipulasi lalu lintas pada antarmuka N2 untuk memicu desinkronisasi nomor sequence dalam prosedur otentikasi 5G-AKA. Hasil eksperimen menunjukkan bahwa intersepsi paket berhasil menyebabkan desinkronisasi nomor sequence, yang secara langsung menyebabkan kegagalan otentikasi dan isolasi perangkat karena Denial of Service. Selain itu, pemantauan jaringan menunjukkan bahwa protokol HTTP/2 menampilkan data pelanggan dalam bentuk teks terang. Sebagai kesimpulan, enkripsi Secure Socket Layer terbukti berhasil sebagai metode mitigasi. Dengan integrasi ini, jalur komunikasi internal telah diubah menjadi format HTTPS yang terenkripsi sepenuhnya, yang mencegah upaya penyadapan. Selain itu, parameter kriptografi pelanggan tetap dilindungi dengan tingkat beban operasional yang masih di bawah toleransi.

**Kata Kunci: Keamanan 5G, Serangan MitM, Desinkronisasi SQN, Open5GS, UERANSIM, SSL/TLS**

## *ABSTRACT*

***ANALYSIS OF 5G STANDALONE SECURITY AGAINST MAN-IN-THE-MIDDLE ATTACKS USING SEQUENCE NUMBER DESYNCHRONIZATION***

**(2026 : XV + 93 *Pages* + 20 *Figures* + 9 *Tables* + 13 *attachment*)**


---


**AN NISA**
**062240352280**
***DEPARTMENT OF ELECTRICAL ENGINEERING***
***BACHELOR OF APPLIED SCIENCE IN TELECOMMUNICATION***
***STATE POLYTECHNIC OF SRIWIJAYA***



*The architectureof standalone 5G networks offers improved communication performance, but its authentication procedures remain vulnerable to eavesdropping threats. This research evaluates the system's vulnerability to Man-in-the-Middle attacks and proposes comprehensive mitigation methods to address these security issues. Relying on Open5GS as the core network and UERANSIM as a simulator for base stations and user devices, testing was conducted in a virtualized environment. The methods used include traffic manipulation at the N2 interface to trigger desynchronization of the sequence number in the 5G-AKA authentication procedure. Experimental results show that packet interception successfully caused sequence number desynchronization, which directly led to authentication failure and device isolation due to Denial of Service. Additionally, network monitoring revealed that the HTTP/2 protocol displays customer data in plain text. In conclusion, Secure Socket Layer (SSL) encryption has proven effective as a mitigation method. With this integration, internal communication channels have been converted to a fully encrypted HTTPS format, preventing eavesdropping attempts. Furthermore, customer cryptographic parameters remain protected while keeping the operational overhead below acceptable limits.*



***Keywords: 5G Security, MitM Attack, SQN Desynchronization, Open5GS, UERANSIM, SSL/TLS***