Implementasi Strategi Keamanan dan Mitigasi Ancaman pada Software Defined Radio (SDR) dengan Simulasi Serangan Nirkabel

Candra Setiawan, Muhammad Gald Teary
Sistem Komputer, Fakultas Ilmu Komputer dan Sains, Universitas Indo Global Mandiri

Jl. Jendral Sudirman No. 629 Km 4 Palembang, Indonesia

Sistem Komputer, Fakultas Ilmu Komputer dan Sains, Universitas Indo Global Mandiri

Jl. Jendral Sudirman No. 629 Km 4 Palembang, Indonesia
candra@uigm.ac.id, m.gald@uigm.ac.id

Abstrak

Software Defined Radio (SDR) merupakan teknologi yang memberikan fleksibilitas tinggi dalam sistem komunikasi nirkabel dengan memungkinkan perangkat keras yang dapat dikonfigurasi ulang dan diprogram melalui perangkat lunak. Fleksibilitas ini memungkinkan berbagai standar komunikasi untuk diadaptasi tanpa memerlukan perubahan pada perangkat keras. Namun, fleksibilitas yang tinggi ini juga membuka potensi besar terhadap berbagai kerentanannya, termasuk serangan *jamming, replay attack, eavesdropping*, dan *spoofing* yang dapat merusak integritas, kerahasiaan, serta ketersediaan data dan sistem. Penelitian ini bertujuan untuk melakukan simulasi terhadap berbagai serangan yang dapat mengancam sistem SDR dan menganalisis efektivitas strategi mitigasi yang diterapkan. Hasil simulasi menunjukkan bahwa proteksi berbasis kriptografi dan autentikasi digital dapat secara signifikan mengurangi potensi gangguan pada sistem. Beberapa rekomendasi yang diusulkan untuk meningkatkan keamanan SDR meliputi validasi digital, pengelolaan sertifikat, manajemen memori, dan deteksi intrusi.

Kata Kunci: *Software Defined Radio*, Keamanan Sistem Informasi*, Jamming*, *Spoofing*, Mitigasi Ancaman

Abstract

Software Defined Radio (SDR) is a technology that provides high flexibility in wireless communication systems by enabling hardware to be reconfigurable and programmable via software. This flexibility allows for the adaptation of various communication standards without requiring modifications to the hardware. However, this high level of flexibility also introduces significant vulnerabilities, including jamming attacks, replay attacks, eavesdropping, and spoofing, which can compromise the integrity, confidentiality, and availability of data and systems. This study aims to simulate various attacks that may threaten SDR systems and analyze the effectiveness of implemented mitigation strategies. The simulation results indicate that cryptographic protection and digital authentication can significantly reduce the potential disruptions to the system. Several recommendations for enhancing SDR security are proposed, including digital validation, certificate management, memory management, and intrusion detection.

Keywords: *Software Defined Radio*, *Information Systems Security, Jamming*, *Spoofing*, *Threat Mitigation*

I. Pendahuluan

Software Defined Radio (SDR) telah menjadi salah satu inovasi penting dalam dunia komunikasi nirkabel, menawarkan fleksibilitas yang luar biasa dalam pengaturan dan interoperabilitas. Dengan SDR, sebagian besar fungsionalitas sistem komunikasi radio kini dapat dikendalikan sepenuhnya melalui perangkat lunak, memungkinkan perangkat untuk beradaptasi dengan berbagai standar komunikasi tanpa memerlukan perubahan pada perangkat keras [1]. Fleksibilitas ini membuat SDR cocok untuk berbagai aplikasi komunikasi, mulai dari kebutuhan pribadi hingga aplikasi industri yang membutuhkan kemampuan untuk mengubah konfigurasi dengan cepat dan efisien.

Namun, keunggulan ini datang dengan tantangan yang tidak kalah besar terkait dengan masalah keamanan. Karena SDR adalah sistem terbuka yang dapat dikonfigurasi ulang, hal ini membuka peluang bagi potensi penyalahgunaan dan serangan dari pihak yang tidak bertanggung jawab, yang pada gilirannya meningkatkan kerentanannya terhadap ancaman luar [2]. Beberapa jenis ancaman yang sering menyerang SDR mencakup *jamming, replay attack, spoofing*, dan *eavesdropping*, yang masing-masing membawa dampak yang berbeda terhadap kualitas sinyal, integritas data, dan kinerja sistem secara keseluruhan. Sebagai contoh, serangan *jamming* dapat menyebabkan gangguan yang serius pada komunikasi, sedangkan *eavesdropping* bisa mencuri data yang sedang dikirim tanpa terdeteksi, yang berisiko besar terhadap privasi.

Tujuan dari penelitian ini adalah untuk mengeksplorasi dampak dari berbagai jenis serangan terhadap sistem SDR menggunakan alat HackRF One dan perangkat lunak GNU Radio pada pita frekuensi 433 MHz. Dengan memahami dampak yang ditimbulkan oleh masing-masing serangan serta langkah mitigasi yang dapat diterapkan, penelitian ini diharapkan dapat memberikan saran yang berguna untuk meningkatkan keamanan sistem SDR. Menurut Fitton (2002), efektivitas strategi mitigasi sangat bergantung pada metode yang diterapkan, termasuk enkripsi yang baik, autentikasi digital yang tepat, serta pengelolaan sertifikat untuk memperkuat sistem SDR [3].

II. Metodologi Penelitian

Penelitian ini menggunakan simulasi yang dilakukan pada sistem SDR dengan memanfaatkan HackRF One dan perangkat lunak GNU Radio pada pita frekuensi 433 MHz, yang sering digunakan dalam komunikasi nirkabel jarak pendek dan relevan dalam konteks SDR. Dalam penelitian ini, kami mensimulasikan empat jenis serangan yang sering terjadi pada SDR, yaitu *jamming, replay attack, spoofing*, dan *eavesdropping*. Tujuan utama dari simulasi ini adalah untuk mengukur dampak dari serangan-serangan tersebut terhadap kekuatan sinyal, kehilangan paket, dan integritas data yang diterima oleh sistem SDR.

A. Jamming

Jamming merupakan serangan yang dirancang untuk mengganggu komunikasi dengan mengirimkan *noise* yang kuat, sehingga mengurangi kualitas sinyal yang diterima dan menyebabkan hilangnya paket data. Dampak dari *jamming* pada sistem SDR cukup signifikan, karena dapat menyebabkan penurunan yang tajam dalam kualitas sinyal dan mengganggu komunikasi. *Jamming* dapat diminimalkan dengan menerapkan teknik seperti *frequency hopping* yang memungkinkan perubahan frekuensi secara dinamis untuk menghindari gangguan sinyal yang ditimbulkan oleh interferensi [4].

B. Replay Attack

Replay attack terjadi ketika data yang sudah ada sebelumnya dikirimkan kembali dengan tujuan mengecoh sistem agar menerima data yang tidak sah. Dalam simulasi ini, kami mengirimkan data dengan *timestamp*

yang sudah kadaluarsa untuk melihat seberapa besar dampaknya terhadap sistem SDR. Serangan ini memanfaatkan kelemahan dalam sistem yang tidak selalu memeriksa keaslian data yang diterima. Penggunaan teknik seperti pengecekan *timestamp* dan penggunaan *nonce* dapat menjadi cara efektif untuk memitigasi risiko *replay attack* pada sistem SDR [5].

C. Spoofing

Spoofing adalah serangan yang dilakukan dengan mengirimkan data palsu yang menggantikan data asli yang sah. Pada simulasi ini, kami mengirimkan data dengan nilai yang tidak sesuai, seperti suhu yang sangat tinggi atau kelembapan yang sangat rendah, yang akan menyebabkan terjadinya kesalahan saat pemeriksaan CRC. Hal ini mengarah pada terjadinya kerusakan dalam integritas data yang diterima. Untuk mencegah *spoofing*, penting bagi sistem SDR untuk menggunakan autentikasi digital yang memastikan bahwa hanya data yang sah yang diterima oleh sistem [2].

D. Eavesdropping

Eavesdropping adalah serangan yang bertujuan untuk menyadap data yang dikirimkan tanpa merubah nilai data tersebut. Meskipun tidak menyebabkan kerusakan langsung pada sistem, *eavesdropping* sangat berbahaya karena dapat mengancam kerahasiaan informasi yang dikirim. Dalam simulasi ini, kami melakukan penyadapan terhadap data yang sedang dikirimkan dan memeriksa apakah data tersebut tetap utuh dan aman. Untuk melindungi data dari serangan ini, dapat menggunakan enkripsi yang kuat, yang dapat memastikan bahwa hanya pihak yang berwenang yang bisa mengakses data yang sensitif [3].

III. Hasil dan Pembahasan

Hasil simulasi menunjukkan bahwa setiap jenis serangan memiliki dampak yang berbeda terhadap performa sistem SDR, baik dalam hal integritas data maupun kekuatan sinyal. Simulasi ini memberikan wawasan penting tentang bagaimana serangan dapat mempengaruhi kinerja sistem dan apa yang dapat dilakukan untuk mengurangi dampaknya.

A Dampak Replay Attack

Replay attack menyebabkan *timestamp* yang salah pada data yang diterima, meskipun data tersebut tetap utuh dan sinyal yang diterima masih kuat. Namun, *timestamp* yang tidak valid dapat mengganggu aplikasi yang bergantung pada data waktu nyata, seperti aplikasi yang membutuhkan data terkini untuk proses keputusan. Meskipun *replay attack* sulit dideteksi secara langsung, masalah ini dapat diatasi dengan pengecekan *timestamp* atau penggunaan *nonce* yang memastikan bahwa data yang diterima adalah data yang sah dan belum pernah dikirim sebelumnya. Penelitian juga menunjukkan bahwa strategi validasi seperti ini efektif dalam mendeteksi *replay attack* dan melindungi integritas sistem SDR [1].

B. Dampak Spoofing

Spoofing menyebabkan integritas data terganggu dengan mengirimkan informasi yang tidak valid, seperti suhu 98°C dan kelembapan 5%. Hal ini mengarah pada *error* pada pemeriksaan *Cyclic Redundancy Check* (CRC), yang menandakan bahwa data yang diterima tidak valid. *Spoofing* merusak keaslian data yang diterima dan dapat menyebabkan sistem tidak dapat diandalkan. Integritas data dalam sistem SDR dapat dilindungi dengan penggunaan teknik autentikasi digital dan pemeriksaan CRC yang lebih ketat untuk memverifikasi kebenaran data yang diterima [2].

C. Dampak Jamming

Jamming memiliki dampak yang sangat merusak terhadap performa sistem, dengan kekuatan sinyal yang sangat lemah (-10 dBm) dan kehilangan paket mencapai 90%. Hal ini menyebabkan *timeout* pada sistem, yang mengganggu aliran komunikasi dan menyebabkan sistem tidak dapat berfungsi dengan baik. Penggunaan teknik *frequency hopping* dapat mengurangi dampak *jamming* dengan mengubah frekuensi transmisi secara dinamis untuk menghindari interferensi [4].

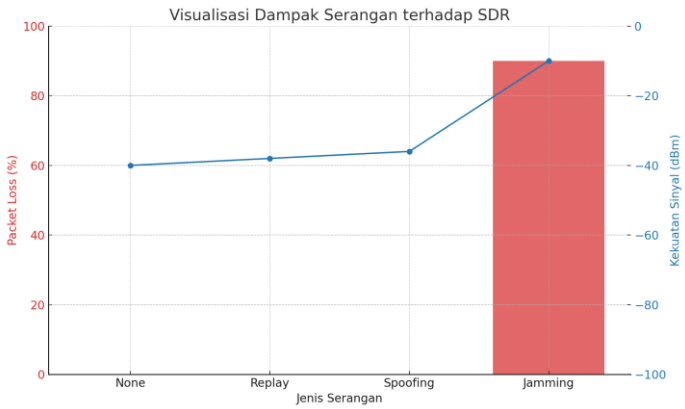
D. Dampak Eavesdropping

Eavesdropping menyebabkan data disadap tanpa mengubah nilai sinyal atau integritas data. Meskipun tidak merusak sistem secara langsung, *eavesdropping* dapat menyebabkan pencurian informasi dan pelanggaran privasi. Penggunaan enkripsi yang kuat dapat melindungi data dari penyadapan dan memastikan bahwa hanya pihak yang berwenang yang dapat mengakses informasi yang dikirimkan [3].

Tabel 1. Dampak Serangan Terhadap Performa SDR

Timestamp	Attack Type	Payload	Signal Strength (dBm)	Packet Loss (%)	Integrity Check
14:02	None	TEMP:27C,HUM:60%,TIME:14:02	-40.0	0.0	Valid
14:03	Replay	TEMP:27C,HUM:60%,TIME:14:02	-38.0	0.0	Invalid Timestamp
14:04	Spoofing	TEMP:98C,HUM:5%,TIME:14:03	-36.0	0.0	CRC Error
14:05	Jamming	No Payload (noise)	-10.0	90.0	Timeout
14:06	Eavesdropping	TEMP:27C,HUM:60% (intercepted)	Nan	nan	N/A

Visualisasi dampak serangan dapat dilihat pada grafik berikut:



Gambar 1. Visualisasi Dampak Serangan Terhadap SDR

IV. Kesimpulan

Hasil simulasi menunjukkan bahwa sistem SDR sangat rentan terhadap berbagai jenis serangan yang dapat mengancam integritas data, kekuatan sinyal, dan keandalan komunikasi. Setiap jenis serangan memiliki dampak yang spesifik yang perlu ditangani dengan strategi mitigasi yang tepat. Dalam menghadapi ancaman tersebut, beberapa langkah mitigasi yang perlu diterapkan meliputi enkripsi payload, autentikasi digital, validasi sertifikat, dan penerapan sistem deteksi intrusi. Teknik mitigasi seperti penggunaan frequency hopping dapat mengurangi dampak dari jamming, sementara

enkripsi yang kuat dapat melindungi data dari penyadapan. Dengan menerapkan strategi mitigasi yang efektif, SDR dapat menjadi lebih aman dan lebih handal dalam menghadapi potensi ancaman yang ada.

REFERENSI

1. Shiba, H., Uehara, K., & Araki, K., "Proposal and evaluation of security schemes for software-defined radio," *Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on*, IEEE, 2003. [Online]. Available: https://www.researchgate.net/publication/4052324_Proposal_and_evaluation_of_security_schemes_for_software-defined_radio.
2. Bhadka, H. B., "GNU Based Security in Software Defined Radio," *International Journal of Computer Applications & Information Technology*, vol. I, issue III, November 2012, pp. 106-113. [Online]. Available: www.ijcait.com.
3. Fitton, J. J., "Security considerations for software-defined radios," *Proceedings of the SDR 02 Technical Conference and Product Exposition*, SDR Forum, 2002, pp. 1-9.
4. Mueck, M., Ivanov, V., Choi, S., Kim, J., Ahn, C., Yang, H., Baldini, G., "Future of wireless communication: RadioApps and related security and radio computer framework," *IEEE Wireless Communications*, vol. 19, no. 8, pp. 10-15, August 2012, doi: 10.1109/MWC.2012.6272418. [Online]. Available: https://www.researchgate.net/publication/260656412.
5. Setiawan, C., & Rahardjo, B., "Potensi ancaman dan analisis kebutuhan keamanan pada Software Defined Radio," *Tugas Akhir Mata Kuliah Keamanan Perangkat Lunak*, Bandung Institute of Technology, 2019. [Online]. Available: https://www.researchgate.net/publication/342549241.