

Performance Evaluation of the Layer 2.5 Zero-Trust Adaptation Layer (ZTAL) Architecture in Tactical UAV Mesh Networks Against Spectrum Attacks

Fujikawa Shinichi^{1*}, Fajar Aziz Kurniawan^{2*}, Fadhil Riyanto^{3*}, Cinantya Paramita^{4*}

* Teknik Informatika, Universitas Dian Nuswantoro

111202415662@mhs.dinus.ac.id¹, 111202415685@mhs.dinus.ac.id², 111202415691@mhs.dinus.ac.id³,
cinantya.paramita@dsn.dinus.ac.id⁴

Article Info

Article history:

Received 2026-07-07

Revised 2026-09-11

Accepted 2026-10-15

Keyword:

Electronic Warfare,
Layer 2.5,
Network Simulator 3,
UAV,
ZTAL.

ABSTRACT

Tactical unmanned aerial vehicle (UAV) mesh networks must maintain useful communication under rapid topology changes, spectrum attack, and traffic pressure. This paper evaluates a Layer-2.5 Zero-Trust Adaptation Layer (ZTAL) as an in-path logical shim between IPv4/OLSR and IEEE 802.11p MAC/PHY. The final experiment uses 90 ns-3 simulations from final_matrix_v3 with Gauss-Markov mobility, 10 and 20 UAV, EDCA, REACTIVE_FH, and ZTAL treatments, and NONE, CW_JAMMING, and ALG_DOS conditions. At 10 UAV under the configured 50 dBm CW jammer, ZTAL improved packet delivery ratio from 57.71% with EDCA to 69.96% (paired difference +12.25 percentage points, Holm $p=1.14e-5$). At 20 UAV, ZTAL improved PDR from 26.83% to 45.95% (paired difference +19.13 percentage points, Holm $p=6.04e-7$). Relative to REACTIVE_FH, ZTAL showed higher mean PDR and more reliable coordination, but the PDR advantage was not statistically conclusive after multiplicity correction with $n=5$. The results also show no-attack overhead, lower delivered byte throughput in several cases, and substantial queue expiry under high-density/load stress. A separate Hard Purge microbenchmark reduced peak protocol-managed reassembly payload state from 192,000 B to 96,020 B under the tested authenticated overlap pattern. The findings support bounded simulation evidence for CW resilience and state-release behavior, not field deployment readiness.



This is an open access article under the [CC-BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.

I. PENDAHULUAN

Jaringan Unmanned Aerial Vehicle (UAV) yang membentuk flying ad hoc network (FANET) menawarkan relai multi-hop tanpa infrastruktur tetap, tetapi mobilitas tinggi, perubahan kanal, dan kontensi MAC membuat komunikasi taktis mudah mengalami degradasi [1]-[4]. Dalam konteks ini, keamanan tidak hanya berarti autentikasi identitas, tetapi juga kemampuan mempertahankan komunikasi berguna ketika media nirkabel terganggu.

Literatur Zero Trust umumnya menekankan identitas, autentikasi, otorisasi, dan kontrol akses [5]-[8], sedangkan penelitian anti-jamming dan cognitive radio banyak membahas adaptasi kanal, topologi, routing, rendezvous, dan survivability spektrum [10]-[13]. Kajian resource exhaustion menempatkan manajemen state sebagai masalah tersendiri

[18]. Literatur yang ditinjau masih memberikan evaluasi terbatas terhadap arsitektur in-path yang menggabungkan autentikasi paket, anti-replay, fragmentasi/reassembly terbatas, pelepasan state overlap terautentikasi, observasi kanal, dan transisi kanal terautentikasi pada mesh UAV IEEE 802.11p.

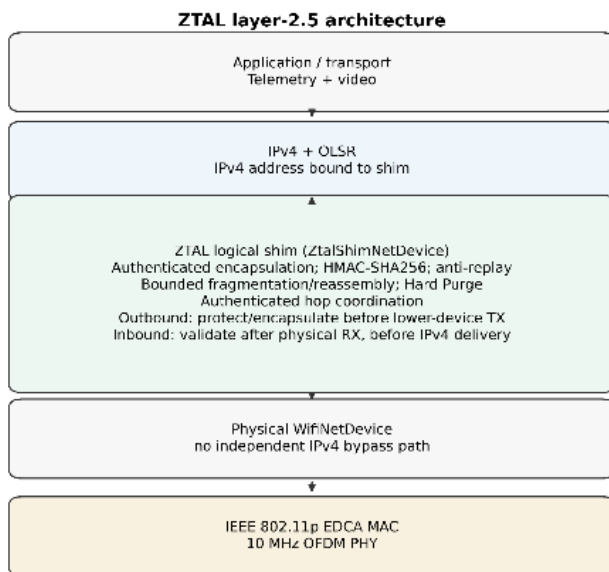
Penelitian ini mengevaluasi Zero-Trust Adaptation Layer (ZTAL) sebagai shim logis pada jalur data antara IPv4/OLSR dan perangkat Wi-Fi IEEE 802.11p. Istilah Layer 2.5 digunakan secara deskriptif untuk posisi arsitektural tersebut; istilah ini bukan lapisan OSI baru, bukan lapisan standar IEEE, dan tidak mengubah model OSI. Kebaruan yang dievaluasi berada pada integrasi dan evaluasi arsitektur, bukan pada HMAC, replay window, atau frequency hopping sebagai teknik individual.

Kontribusi penelitian meliputi: evaluasi ZTAL sebagai shim in-path pada mesh UAV IEEE 802.11p; pemrosesan paket terautentikasi dan replay protection sebelum delivery ke Layer 3; fragmentasi dan reassembly terautentikasi dengan batas sebelum alokasi; Hard Purge untuk state overlap terautentikasi; koordinasi transisi kanal berbasis detector CCA_BUSY; perbandingan terhadap EDCA non-hopping dan REACTIVE_FH; serta analisis $n=5$ berbasis simulation run dengan CI, uji berpasangan, QoS-class analysis, dan temuan negatif eksplisit. Studi keamanan data-link dan monitoring drone lokal tetap relevan sebagai konteks aplikasi, tetapi tidak menjadi klaim hasil eksperimen ZTAL [19], [20].

II. METODE

A. Arsitektur ZTAL dan Justifikasi Layer 2.5

Gambar 1 menunjukkan posisi ZTAL. Aliran Application/UDP dan IPv4+OLSR melewati ZtalShimNetDevice sebelum diteruskan ke WifiNetDevice fisik dan MAC/PHY IEEE 802.11p. IPv4 diberikan pada perangkat shim logis, sedangkan perangkat Wi-Fi bawah tidak memiliki jalur IPv4 independen yang dapat melewati perlindungan ZTAL.



Gambar 1. Posisi logis ZTAL sebagai shim in-path antara IPv4/OLSR dan IEEE 802.11p MAC/PHY.

Secara semantik, ZTAL menerapkan authenticated encapsulation pada arah outbound sebelum transmisi oleh perangkat bawah. Pada arah inbound, autentikasi dan replay validation terjadi setelah frame diterima secara fisik, tetapi sebelum paket diserahkan ke IPv4/Layer 3. Formulasi ini sengaja menghindari klaim yang keliru bahwa frame inbound dapat diverifikasi secara kriptografis sebelum penerimaan fisik.

ZTAL menggunakan HMAC-SHA256 dengan kunci simulasi 256-bit deterministik yang telah diprovisikan sebelumnya, Security Association, tag autentikasi

tertransmisi 128-bit, replay window 64 entry, fragmentasi terautentikasi, reassembly terbatas, pre-allocation rejection, Hard Purge, dan koordinasi hop terautentikasi. Tidak ada confidentiality, enkripsi, key exchange, atau credential recovery yang dimodelkan sebagai properti final.

Frozen source menetapkan ZtalHeader::SERIALIZED_SIZE sebesar 52 byte: Magic 4 B, Version 1 B, Flags 1 B, Header Length 2 B, SPI 4 B, Sequence 8 B, Message ID 4 B, Fragment Offset 4 B, Fragment Length 2 B, Reserved 2 B, Total Message Length 4 B, dan Authentication Tag 16 B. Ukuran inner packet legal maksimum adalah 1.500 byte. State reassembly dibatasi 128 context dan 192.000 byte protocol-managed reassembly payload per node, dengan metadata fragment-receipt fixed-size berupa bitmap 1.500 byte receipt per context yang diimplementasikan menggunakan `std::bitset<1500>`.

Batas 128 context/192.000 byte tidak dipilih dari hasil performa final. Pilot cadangan 64 context/96.000 byte masih menimbulkan legitimate context-limit rejection, sedangkan kandidat pre-registered pertama yang digandakan menjadi 128 context/192.000 byte menghilangkan byte/context allocation-limit rejection pada lima nominal pilot. Maksimum pilot tercatat 85.212 byte dan 81 context.

B. Desain Eksperimen, Mobilitas, dan Workload

Eksperimen final menggunakan ns-3 dengan IEEE 802.11p 10 MHz, DataMode OfdmRate24MbpsBW10MHz, ControlMode Ofdm Rate 6 Mbps BW 10 MHz, initial Channel 172 pada 5860 MHz, dan configured alternate Channel 180 pada 5900 MHz. Implementasi spektrum memakai MultiModelSpectrumChannel dengan constant-speed propagation delay, Friis spectrum propagation component, dan Nakagami fading component. Channel 180 adalah kanal alternatif terkonfigurasi, bukan hasil pencarian kanal arbitrer, reinforcement learning, atau optimasi spektrum real-time. Channel 180 ditetapkan sebagai kanal alternatif tetap, penelitian ini tidak mengevaluasi optimalitas pemilihan kanal tujuan.

Topologi adalah mobile mesh pada area horizontal 250 m x 250 m dengan altitude 50-150 m. Mobilitas menggunakan Gauss-Markov, speed Uniform[25,35] m/s, alpha 0.85, dan TimeStep 0.5 s. Kondisi 10 UAV adalah operational condition utama, sedangkan 20 UAV adalah high-density/load stress evaluation karena node count, density, aggregate offered traffic, dan contention berubah bersamaan.

Setiap UAV menghasilkan telemetry 50 Kbps dengan 64-byte application payload, DSCP CS6, UP6, AC_VO; serta video 500 Kbps dengan 1024-byte application payload, DSCP CS4, UP4, AC_VI. Offered application load adalah 550 Kbps per UAV, 5.5 Mbps untuk 10 UAV, dan 11 Mbps untuk 20 UAV. NeighborCacheHelper prepopulation digunakan pada semua treatment untuk menghilangkan synchronized ARP startup artifacts; ini bukan optimisasi khusus ZTAL.

TABEL 1.

PARAMETER SIMULASI FINAL YANG DIGUNAKAN PADA FINAL_MATRIX_V3

Parameter	Final configuration
Network/PHY	IEEE 802.11p, 10 MHz
Data/control mode	24 Mbps / 6 Mbps
Channel	172=5860 MHz; 180=5900 MHz
Mobility	Gauss-Markov, 250 m x 250 m, 50-150 m
Traffic	Telemetry 50 Kbps AC_VO; video 500 Kbps AC_VI
Matrix	3 protocols x 3 attacks x 2 scales x 5 runs
Seed/duration	RngSeed 12345; RngRun 1-5; 300 s

C. Treatment Protokol dan Frequency Hopping

EDCA adalah baseline QoS IEEE 802.11p non-hopping dengan PHY, mobilitas, workload, OLSR, QoS, channel model, dan neighbor-cache mode yang sama, tetapi tanpa perlindungan ZTAL dan tanpa frequency hopping. REACTIVE_FH memakai detector jammer yang sama dengan ZTAL dan alur detection, request, acknowledgement, commit, switch, tetapi koordinasinya tidak terautentikasi. Transisi REACTIVE_FH tidak memiliki delay tetap yang dipredeterminasikan; keberhasilan koordinasi dan retry menentukan waktu peralihan.

ZTAL memakai detector yang sama dengan REACTIVE_FH, tetapi koordinasi hop dilindungi. Setelah threshold terlampaui, ZTAL membentuk hop announcement terautentikasi yang memuat coordination epoch, source channel, target channel, scheduled switch time, per-message nonce, origin node, dan authentication tag. Peer menerima koordinasi hanya setelah autentikasi berhasil, kemudian melakukan transisi dari Channel 172 ke Channel 180 pada waktu terjadwal.

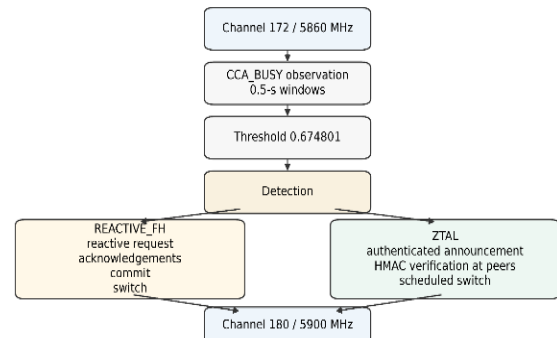
TABEL 2.

PERBANDINGAN FITUR TREATMENT PROTOKOL; DETECTOR REACTIVE_FH DAN ZTAL IDENTIK

Feature	EDCA	REACTIVE_FH	ZTAL
QoS AC_VO/AC_VI	Yes	Yes	Yes
Common CCA_BUSY detector	No hop	Yes	Yes
Frequency transition	No	Reactive	Authenticated event-driven
Coordination authentication	-	No	Yes
In-path auth/replay	No	No	Yes
Bounded reassembly/Hard Purge	No	No	Yes

Jammer detection and channel transition

Configured alternate channel: 180. Adaptivity is event-driven detection and transition, not online multi-channel optimization.



Gambar 2. Alur detector CCA_BUSY dan transisi kanal terkoordinasi.

D. Threat Model, Detector, dan Statistik

Detector tidak mengetahui attackType, identitas jammer, atau waktu mulai jammer. Observable adalah aktual PHY CCA_BUSY occupancy pada window 0.5 s. Threshold beku 0.674801 dipilih dari kalibrasi yang memisahkan maksimum NONE 0.350334 dan minimum active-CW 0.999268; PDR dan throughput tidak digunakan untuk tuning threshold.

Tiga kondisi utama digunakan. NONE mengukur overhead tanpa serangan. CW_JAMMING menggunakan continuous-wave jammer 50 dBm atau sekitar 100 W pada Channel 172. ALG_DOS adalah attacker UDP berkecepatan tinggi yang memberi tekanan jaringan/MAC untuk mengekspos contention, queue pressure, retry, dan degradasi aplikasi. ALG_DOS bukan eksperimen Hard Purge.

Hard Purge diuji secara terpisah melalui microbenchmark fragmen overlap terautentikasi. Peer malicious memiliki material autentikasi valid dan sengaja membuat overlap fragment. Dengan pemisahan ini, hasil Hard Purge tidak ditafsirkan sebagai bukti dari ordinary ALG_DOS.

Unit eksperimen adalah simulation run, bukan paket. Matriks final berisi 90 simulasi valid: EDCA, REACTIVE_FH, ZTAL; NONE, CW_JAMMING, ALG_DOS; 10 dan 20 UAV; RngRun 1-5; RngSeed 12345; durasi 300 s; traffic start 1 s. Setiap cell dilaporkan sebagai mean dan 95% Student-t CI dengan n=5. Analisis terencana memakai blok RngRun berpasangan, paired mean difference, paired-difference 95% CI, paired t-test, Wilcoxon signed-rank sensitivity analysis, Cohen dz bila sesuai, dan Holm multiplicity correction. Keterbatasan n=5 tetap eksplisit.

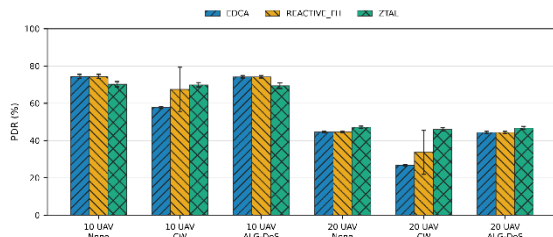
III. HASIL DAN PEMBAHASAN

TABEL 3.

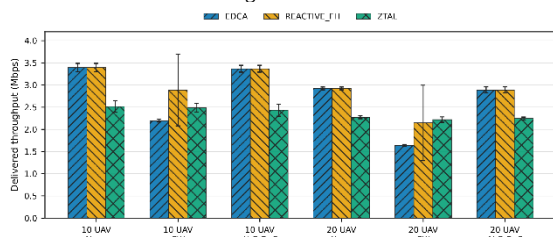
RINGKASAN PDR UTAMA, MEAN +/- 95% STUDENT-T CI HALF-WIDTH, N=5 SIMULATION RUNS

Condition	EDCA	REACTIVE_FH	ZTAL
NONE, 10 UAV	74.41 +/- 1.14%	74.41 +/- 1.14%	70.25 +/- 1.39%
CW_JAMMING, 10 UAV	57.71 +/- 0.58%	67.49 +/- 11.84%	69.96 +/- 1.18%
ALG_DOS, 10 UAV	74.22 +/- 0.67%	74.22 +/- 0.67%	69.39 +/- 1.46%

NONE, 20 UAV	44.61 +/- 0.40%	44.61 +/- 0.40%	47.16 +/- 0.54%
CW_JAMMIN G, 20 UAV	26.83 +/- 0.30%	33.62 +/- 11.79%	45.95 +/- 0.84%
ALG_DOS, 20 UAV	44.32 +/- 0.55%	44.32 +/- 0.55%	46.74 +/- 0.79%



Gambar 3. Packet Delivery Ratio menurut protokol, kondisi, dan skala dengan 95% CI.



Gambar 4. Delivered application throughput dengan 95% CI.

A. Overhead pada Kondisi NONE

Pada NONE 10 UAV, EDCA mencapai PDR 74.41 +/- 1.14%, throughput 3.392 +/- 0.092 Mbps, dan delay 165.43 +/- 5.49 ms. ZTAL menghasilkan PDR 70.25 +/- 1.39%, throughput 2.514 +/- 0.130 Mbps, dan delay 176.87 +/- 12.52 ms. Paired difference ZTAL-EDCA adalah -4.16 +/- 1.37 percentage point, sehingga overhead tanpa serangan harus dipertahankan sebagai temuan negatif.

Pada NONE 20 UAV, packet-level PDR ZTAL lebih tinggi daripada EDCA, tetapi delivered byte throughput ZTAL tetap lebih rendah. Ini menunjukkan bahwa PDR paket dan throughput byte tidak selalu bergerak sama ketika paket kecil berprioritas tinggi lebih sering bertahan daripada paket video besar.

B. Resiliensi dan Koordinasi pada CW Jamming

CW_JAMMING menurunkan EDCA secara tajam. Pada 10 UAV, EDCA memperoleh PDR 57.71 +/- 0.58% sedangkan ZTAL 69.96 +/- 1.18%; paired difference adalah +12.25 +/- 0.96 percentage point dengan Holm $p=1.14e-05$. Pada 20 UAV, EDCA 26.83 +/- 0.30% dan ZTAL 45.95 +/- 0.84%; paired difference +19.13 +/- 0.72 percentage point dengan Holm $p=6.04e-07$.

Dibanding REACTIVE_FH, ZTAL memiliki mean PDR lebih tinggi dan koordinasi lebih andal, tetapi PDR advantage tidak statistically conclusive setelah multiplicity correction dengan $n=5$. Pada CW 10 UAV, ZTAL-REACTIVE_FH adalah +2.47 +/- 12.22 percentage point dengan Holm $p=0.605$. Pada CW 20 UAV, paired t p mentah lebih kecil, tetapi Holm $p=0.0915$ tetap di atas ambang 0.05.

TABEL 4.

PAIRED PDR CONTRASTS UTAMA; WILCOXON SENSITIVITY TERBATAS OLEH $N=5$

Contrast	dPDR pp	Holm p	Interpretation
CW10 ZTAL-EDCA	+12.25 +/- 0.96	1.14e-05	consistent
CW20 ZTAL-EDCA	+19.13 +/- 0.72	6.04e-07	consistent
CW10 ZTAL-RFH	+2.47 +/- 12.22	0.605	not conclusive
CW20 ZTAL-RFH	+12.33 +/- 11.96	0.092	not conclusive

Reliabilitas koordinasi menjelaskan sebagian mekanisme. ZTAL berhasil melakukan hop pada 5/5 run untuk 10 UAV dan 5/5 run untuk 20 UAV dengan detection-to-hop latency sekitar 0.1005 s. REACTIVE_FH hanya sukses pada 3/5 run di 10 UAV dan 2/5 run di 20 UAV; successful-run latency sekitar 0.5676 s dan 0.4005 s. Run gagal tersebut tidak disembunyikan karena menjadi sumber CI yang besar.

Keuntungan CW dibayar dengan queue pressure. Pada CW 10 UAV, queue-lifetime expiry ZTAL 316349 +/- 13102 dibanding EDCA 188606 +/- 2582. Pada CW 20 UAV, ZTAL 1093028 +/- 12281 dibanding EDCA 677234 +/- 2487. Authenticated fragmentation dan workload data-plane tambahan meningkatkan MAC workload dan queue-lifetime expiration, terutama pada density/load stress.

C. QoS Telemetry dan Video

Pemisahan kelas trafik menjelaskan mengapa ZTAL dapat menaikkan packet-level PDR tetapi menurunkan delivered byte throughput. Pada ZTAL/NONE 10 UAV, telemetry PDR 88.25 +/- 0.83% sedangkan video 41.45 +/- 2.54%. Pada ZTAL/CW 10 UAV, telemetry 88.09 +/- 0.92% dan video 40.94 +/- 1.88%. Pada ZTAL/CW 20 UAV, telemetry masih 64.86 +/- 1.13% tetapi video turun menjadi 15.71 +/- 0.53%. Paket telemetry kecil dengan AC_VO bertahan jauh lebih kuat daripada paket video besar AC_VI.

Perilaku QoS ini tidak diatribusikan pada Adaptive Integer Token Bucket. final_matrix_v3 tidak menyediakan ablation AITB ON/OFF, sehingga efek isolated AITB tidak dievaluasi dan tidak menjadi klaim novelty tervalidasi. Treatment QoS final yang diuji adalah klasifikasi EDCA AC_VO dan AC_VI.

D. ALG_DOS dan High-Density/Load Stress

ALG_DOS tidak menghasilkan kemenangan universal. Pada 10 UAV, EDCA memperoleh PDR 74.22 +/- 0.67% dan throughput 3.366 +/- 0.077 Mbps, sedangkan ZTAL 69.39 +/- 1.46% dan 2.431 +/- 0.135 Mbps. Pada 20 UAV, PDR ZTAL sedikit lebih tinggi daripada EDCA, tetapi byte throughput tetap lebih rendah. ALG_DOS terutama mengekspos MAC/queue pressure, retry, dan degradasi aplikasi, bukan efektivitas Hard Purge.

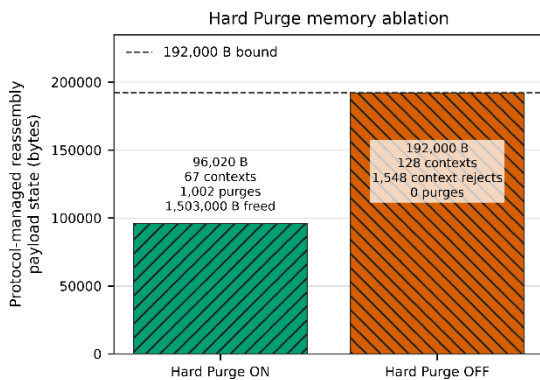
Perubahan 10 ke 20 UAV tidak boleh disebut pure

constant-load scalability experiment. Node count, node density, aggregate offered load, dan contention meningkat bersamaan dari 5.5 Mbps menjadi 11 Mbps. Semua treatment mengalami degradasi PDR. ZTAL/CW turun sekitar 24.00 +/- 1.81 percentage point, sedangkan EDCA/CW turun sekitar 30.89 +/- 0.84 percentage point. Interpretasi yang tepat adalah high-density/load stress evaluation.

E. Evaluasi Terpisah Hard Purge

TABEL 5.
MICROBENCHMARK HARD PURGE TERHADAP FRAGMEN OVERLAP
TERAUTENTIKASI; TERPISAH DARI ALG_DOS

Metric	Hard Purge ON	Hard Purge OFF
Peak payload B	96020	192000
Peak contexts	67	128
Time >=90% bound s	0.0	1.65
Byte/context rejects	0 / 0	0 / 1548
Overlaps/purges	1002 / 1002	992 / 0
Bytes freed	1503000	0
Legit PDR %	61.83	60.85



Gambar 5. Peak protocol-managed reassembly payload pada Hard Purge ON/OFF.

Dengan Hard Purge ON, peak protocol-managed reassembly payload adalah 96.020 byte, peak context 67, time >=90% configured bound 0 s, byte/context reject 0/0, authenticated overlaps 1.002, purges 1.002, dan bytes freed 1.503.000. Legitimate PDR adalah 61.83%, delay 222.73 ms, dan throughput 1.916 Mbps.

Dengan Hard Purge OFF, state mencapai 192.000 byte dan 128 context, time >=90% bound 1.65 s, context reject 1.548, overlap 992, purge 0, dan bytes freed 0. Legitimate PDR 60.85%, delay 223.36 ms, dan throughput 1.789 Mbps. Interpretasinya sempit: Hard Purge mendukung state-release protection terhadap pola overlap terautentikasi yang diuji, bukan perlindungan universal dari semua memory attack.

F. Routing, Bandwidth, dan Keterbatasan

Instrumentasi final mencakup routing trace events, jumlah node dengan final routing table kosong, FlowMonitor forwarding events, forwarding-events per source packet, dan forwarding-events per delivered packet. timesForwarded

tidak disebut average hop count. Routing-control-byte overhead OLSR tidak diukur sebagai metrik khusus, sehingga pembahasan dibatasi pada routing activity dan forwarding-event burden.

Bandwidth yang dilaporkan adalah delivered application throughput. PHY airtime dan channel occupancy dipakai sebagai diagnostik channel work dan retransmission pressure, bukan energy consumption. Tidak ada radio-energy model tervalidasi pada final_matrix_v3, sehingga tidak ada klaim Joule atau energi UAV.

Validitas eksternal dibatasi oleh simulator ns-3 dan ketiadaan RF hardware nyata. Jammer yang diuji adalah CW 50 dBm pada Channel 172; weak, intermittent, reactive, sweep, deceptive jammer, selective forwarding, dan variasi partial jammer observability belum diuji. Real radio clock drift, oscillator imperfection, antenna orientation/non-linearity, dan implementation latency dapat berbeda. HMAC CPU processing delay saat ini nol di simulasi; host wall-clock time bukan cryptographic latency. Tidak ada process RSS atau allocator-overhead claim. Kunci deterministik telah diprovisikan sebelumnya; tidak ada key exchange, credential recovery, confidentiality, atau klaim kesiapan implementasi lapangan. Ukuran sampel n=5 tetap kecil meskipun CI dan paired analysis membantu transparansi ketidakpastian.

IV. KESIMPULAN

Eksperimen final menunjukkan bahwa ZTAL sebagai shim in-path Layer-2.5-style meningkatkan resilience terhadap configured CW jammer dibanding EDCA non-hopping pada 10 dan 20 UAV. Koordinasi terautentikasi ZTAL lebih reliable daripada REACTIVE_FH pada run final, tetapi PDR superiority terhadap REACTIVE_FH tidak statistically conclusive setelah multiplicity correction dengan n=5.

Manfaat tersebut memiliki biaya. Pada NONE 10 UAV, ZTAL menunjukkan overhead PDR dan throughput. Pada high-density/load stress 20 UAV, queue pressure meningkat besar dan delivered byte throughput sering lebih rendah karena telemetry kecil bertahan jauh lebih kuat daripada video besar. ALG_DOS menghasilkan hasil campuran dan tidak boleh ditafsirkan sebagai kemenangan universal.

Microbenchmark Hard Purge mendukung perlindungan bounded reassembly state terhadap tested authenticated overlap pattern, dengan pelepasan state yang jelas saat purge aktif. Namun simulasi ini tidak menetapkan kesiapan implementasi lapangan. Validasi hardware/RF, energy model, broader jammer models, key-management design, processing latency kriptografis, dan eksperimen dengan jumlah run lebih besar tetap menjadi pekerjaan lanjutan.

DAFTAR PUSTAKA

- [1] A. Hussain, S. Li, T. Hussain, X. Lin, F. Ali, and A. A. AlZubi, "Computing Challenges of UAV Networks: A Comprehensive Survey," *Computers, Materials & Continua*, vol. 81, no. 2, pp. 2457-2496, 2024.
- [2] Z. Zhou, J. Tang, W. Feng, N. Zhao, Z. Yang, and K. Wong,

- "Optimized Routing Protocol Through Exploitation of Trajectory Knowledge for UAV Swarms," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 5, pp. 6961-6976, 2024.
- [3] A. Shafique, A. Mehmood, and M. Elhadeif, "Survey of Security Protocols and Vulnerabilities in Unmanned Aerial Vehicles," *IEEE Access*, vol. 9, pp. 46931-46948, 2021.
- [4] D. Shumeye Lakew, U. Sa'Ad, N. N. Dao, W. Na, and S. Cho, "Routing in Flying Ad Hoc Networks: A Comprehensive Survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1071-1120, 2020.
- [5] H. Kang, G. Liu, Q. Wang, L. Meng, and J. Liu, "Theory and Application of Zero Trust Security: A Brief Survey," *Entropy*, vol. 25, no. 12, art. 1595, 2023, doi: 10.3390/e25121595.
- [6] C. Buck, C. Olenberger, A. Schweizer, F. Volter, and T. Eymann, "Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-trust," *Computers & Security*, vol. 110, art. 102436, 2021.
- [7] K. Ramezanzpour and J. Jagannath, "Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN," *Computer Networks*, vol. 217, art. 109358, 2022.
- [8] X. Qu, W. Ou, M. Pang, Y. Chen, Y. Wu, Q. Yue, and W. Han, "A Lightweight Zero-Trust-Based Authentication Framework for UAV Systems," *Sensors*, vol. 26, no. 13, art. 4161, 2026.
- [9] D. Mallikarachchi, K. S. Wong, and J. M. Y. Lim, "An authentication scheme for FANET packet payload using data hiding," *Journal of Information Security and Applications*, vol. 76, art. 103545, 2023.
- [10] C. Pu, "Jamming-Resilient Multipath Routing Protocol for Flying Ad Hoc Networks," *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2879758.
- [11] T. T. Sari and G. Secinti, "Using Centrality Based Topology Control for FANET Survivability Against Jamming," *Computer Networks*, art. 110250, 2024, doi: 10.1016/j.comnet.2024.110250.
- [12] L. Cheng, Z. Xu, J. Zhou, D. Tian, X. Duan, K. Qu, and A. Zhao, "Adaptive Spectrum Anti-Jamming in UAV-Enabled Air-to-Ground Networks: A Bimatrix Stackelberg Game Approach," *Electronics*, vol. 13, no. 19, art. 3958, 2024.
- [13] Y.-H. Hsieh, C.-M. Chao, C.-Y. Lin, and C.-C. Yeh, "Anti-Jamming Low-Latency Channel Hopping Protocol for Cognitive Radio Networks," *Electronics*, vol. 12, no. 8, art. 1811, 2023.
- [14] M. G. Spina, M. Tropea, and F. De Rango, "SURA-LB: Software-defined IDS with UAV Resource Aware Load-Balancing in FANET disaster scenarios," *Computer Communications*, vol. 223, pp. 160-173, 2024.
- [15] L. Ismail, D. Uomo, A. Sgambelluri, F. Alhamed, and F. Paolucci, "P4 FANET In-band Telemetry (FINT) for AI-assisted wireless link failure forecasting and recovery," *Computer Networks*, art. 110712, 2025.
- [16] M. T. Naser and A. H. Wheeb, "Implementation of RWP and Gauss Markov Mobility Model for Multi-UAV Networks in Search and Rescue Environment," *International Journal of Interactive Mobile Technologies*, vol. 18, no. 18, pp. 54-68, 2024.
- [17] X. Lei, X. Chen, and S. H. Rhee, "A hybrid access method for broadcasting of safety messages in IEEE 802.11p VANETs," *EURASIP Journal on Wireless Communications and Networking*, vol. 2018, art. 230, 2018.
- [18] V. Desnitsky, I. Kotenko, and D. Zakoldaev, "Evaluation of Resource Exhaustion Attacks against Wireless Mobile Devices," *Electronics*, vol. 8, no. 5, art. 500, 2019, doi: 10.3390/electronics8050500.
- [19] R. Fachrurzy, M. Y. B. Setiadji, and D. F. Priambodo, "Embedded WIDS Kismet Sebagai Perangkat Deteksi Serangan Data Link Layer Wi-Fi Access Point," *Jurnal Informatika: Jurnal Pengembangan IT*, vol. 9, no. 2, pp. 88-95, 2024.
- [20] R. S. Wijaya, R. A. Fatekha, N. Nazhifah, and Y. A. Mubarak, "Design of a Real-Time Wireless-Based Flight Monitoring and Drone Surveillance System," *Journal of Applied Informatics and Computing*, vol. 8, no. 2, pp. 290-297, 2024.
- [21] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," *NIST Special Publication 800-207*, National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-207.