Analisa Efesiensi Energy Menggunakan Protocol Hybrid Dalam Jaringan Ad hoc

Hariani Ma'tang Pakka[1,a)], Tanridio Silviati Delfina Abdurrahman[2,b)], Salmiah[3,c)], Saidah Suyuti[4,d)], Sriwijanaka Yudi Hartono[5,e)], Muhammad Anas Masa[6,f)]

[1,2,3,4,5,6]Program Studi Teknik Elektro, Fakultas Teknik, Universitas Muslim Indonesia

email: hariani.m@umi.ac.id[a)], tanridiosiviati.da@umi.ac.id[b)], salmiah.salmiah@umi.ac.id[c)] saidah.suyuti@umi.ac.id[d)], sriwijanaka.hartono@umi.ac.id[e)], anas.masa@umi.ac.id[f)]

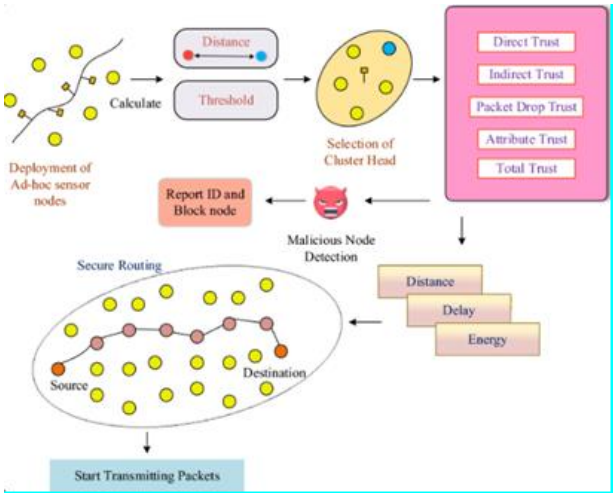
Abstract

Jaringan Ad Hoc adalah jenis jaringan nirkabel yang terbentuk secara spontan dan sementara antara perangkat yang saling terhubung tanpa memerlukan infrastruktur tetap seperti titik akses atau router. Meskipun jaringan ad hoc menawarkan fleksibilitas, mobilitas node yang terus-menerus membuatnya rentan terhadap serangan privasi. Keamanan menjadi fokus utama dalam Internet of Things (IoT) karena kerangka kerja yang fleksibel, dan ancaman seperti modifikasi perangkat lunak dan spionase dapat muncul. Pentingnya mendeteksi intrusi dalam jaringan ad hoc menjadi krusial untuk melindungi privasi dan menyediakan perlindungan. Pengawasan invasi adalah metode terbaik untuk mengidentifikasi potensi pelanggaran lebih lanjut. Selain itu, hilangnya sumber energi dari node dapat mempengaruhi kapasitas stasiun seluler, yang memerlukan pengembangan protokol sebagai metode pilihan koneksi terbaik dan paling dapat diandalkan. Pendekatan hibrida diimplementasikan dengan menggabungkan algoritma Cat Slapped Solo Algorithm (C-SSA) untuk memilih langkah-langkah optimal dalam pengembangan rute. Penggunaan pengelompokan fuzzy dan pemilihan Cluster Head (CH) berdasarkan signifikansi kepercayaan memberikan dasar untuk perutean multi-hop nirkabel. Algoritma hibrida ini menawarkan kepercayaan dalam aspek keamanan dan efisiensi energi saat perjalanan di dalam jaringan ad hoc. Hasil eksperimen menunjukkan bahwa metode yang diusulkan menghasilkan kebutuhan energi yang rendah, durasi minimum, kecepatan pemahaman dan penyelesaian yang tinggi, persentase terbesar untuk paket data, dan tingkat deteksi yang baik. Teknik ini juga dibandingkan dengan metode yang sudah ada, termasuk yang melibatkan serangan pada model pelompatan paket selektif, menunjukkan keunggulannya dalam menghadapi tantangan keamanan dan efisiensi energi dalam konteks jaringan ad hoc.

Keywords: *Jaringan Ad Hoc, Internet of Things (IoT), Pengawasan Intrusi, Protokol Energi Efisien, Algoritma Cat Slapped Solo (C-SSA)*

I. PENDAHULUAN

Konektivitas telepon dalam jaringan ad hoc melibatkan node yang terhubung secara nirkabel dalam kedua arah, dan setiap node berperan sebagai penerima dan pemancar radio. Faktor utama yang memungkinkan transmisi data di seluruh properti dengan karakteristik yang sebanding dan menjaga keefektifan jaringan ad hoc. System transfer ini menyebabkan terbatasnya cakupan siaran, sehingga menantang bagi banyak node untuk berbagi data di seluruh platform. Keandalan mungkin menjadi tantangan signifikan dalam jaringan Wi-Fi yang beroperasi secara ad hoc karena node yang dapat dipindahkan bergantung pada baterai. Baterai ini memiliki keterbatasan daya dan sulit untuk diisi ulang atau diperbarui dalam banyak situasi [1]. Peralatan elektronik tetap menjadi perhatian utama, meskipun ada kemajuan dalam penyimpanan energi. Diperlukan penelitian lebih lanjut terhadap metode yang efektif, media, dan desain inovatif. Dengan mempertimbangkan masa pakai yang terbatas dari sumber daya tersebut, kegunaan sistem informal sangat dibatasi oleh kemampuan akses.



Gambar 1. Rute energy efesiensi Protocol Hybrid Dalam Jaringan ad hoc[2]

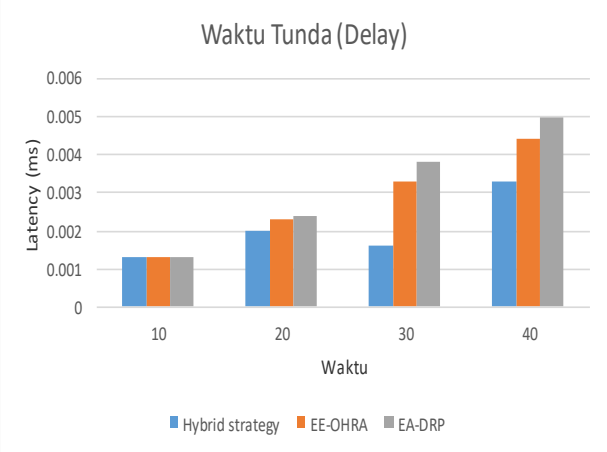
Komunikasi merupakan salah satu penggunaan utama daya listrik. Dengan laju pengembangan operasi baterai yang sekarang sangat lambat karena kurangnya kemajuan di sektor ini, langkah-langkah lebih lanjut diperlukan untuk mencapai efisiensi yang lebih baik, terutama karena aset baterai saat ini mudah diakses. Ketika port radio pada node sel diblokir, yang dapat terjadi kapan saja, penggunaan energi meningkat, bahkan ketika simpul sel menggunakan paket, saat sedang beristirahat, atau dalam keadaan tidur. Instrumen yang digunakan dalam sistem sel ad hoc dan sistem premis ad hoc perlu memiliki fleksibilitas karena mereka dapat dipindahkan dan harus bersaing dengan batasan massa, ukuran, dan ketersediaan sumber daya [3]. Kapasitas baterai yang ditingkatkan dapat membuat node menjadi lebih berat dan kurang portabel. Oleh karena itu, perutean terus menekankan efisiensi hidup sebagai faktor desain kunci.

Terdapat banyak risiko yang dapat memengaruhi perangkat bersama dengan telekomunikasi publik lainnya. Ancaman potensial melibatkan baik perangkat yang rusak secara internal maupun penyusup eksternal. Untuk melindungi sistem semacam ini, diperlukan berbagai solusi keamanan informasi, seperti perlindungan kata sandi, administrasi identitas, dan pencegahan penyusupan. Penggunaan akses broadband dan kemampuan beradaptasi dari peralatan yang berbeda dapat memiliki konsekuensi negatif, dan sejumlah pendekatan deteksi umum serta solusi yang tidak langsung dapat tidak terdeteksi pada platform sistem IP. Selain itu, bersamaan dengan potensi serangan kecepatan dan telepon digital, kemungkinan serangan Man in the Middle dan serangan impersonasi pada infrastruktur juga telah berkembang [4]. Karena potensi transfer paket yang tidak efektif, risiko alarm palsu dan tuduhan palsu terhadap stasiun di jaringan cukup signifikan. Potensi ini muncul dari pergerakan di dalam sistem yang mengganggu transmisi dan melalui sejumlah mekanisme. Selain itu, tidak ada lokasi kritis dalam sistem, seperti sakelar, gerbang, atau dinding di Internet yang terhubung protokol, di mana semua pengunjung yang berwenang dapat diidentifikasi dan dinilai untuk mendeteksi perilaku berbahaya.

Tujuan dari penelitian ini adalah mengembangkan suatu rute berbasis algoritma campuran yang aman untuk jaringan Ad-hoc. Cluster fuzzy pertama kali diaktifkan, dan kepala cluster dipilih berdasarkan tingkat terbesar dari kepercayaan tidak langsung, langsung, dan kontemporer. Node yang memenuhi ambang batas kepercayaan yang ditentukan juga diidentifikasi. Bahkan CH turut serta dalam perutean multi-hop, dengan pemilihan jalur tergantung pada algoritma hibrid yang direkomendasikan, menentukan rute optimal berdasarkan metode optimasi [5]. Pendekatan optimasi ini berfungsi sebagai fungsi dari jumlah energi yang tersisa dalam sirkuit, kapasitas rute, dan konektivitas atau aksesibilitas rute. Korelasi Wiggly digunakan pada tahap awal untuk memilih CH dalam area jaringan ad hoc dengan keseimbangan yang tepat antara implisit, instruktif, dan harapan kontemporer. Detektor gangguan digunakan untuk mendeteksi node yang melanggar untuk paket yang terus menerus ditransmisikan dari sumber ke tujuan. Semua langkah konstruktif perutean dan sistem otomatis fusi yang diperoleh dari konektivitas pengoptimal salp ini diikuti dengan sangat cermat. Untuk operasi tujuan yang ditegaskan, kapasitas, kecepatan, dan kontak di sepanjang jalur ini menjadi penting. Manfaat dari SSA dan pendekatan Cos digabungkan dalam algoritma yang diusulkan, dan diharapkan bahwa langkah-langkah penambangan dan manipulasi algoritme ini akan berjalan dengan baik. Hasil akan dievaluasi berdasarkan apakah simulasi mampu menangkap penurunan paket.

II. Tinjauan Pustaka

Pembatasan kinerja sel ini memiliki dampak pada ketahanan jaringan secara keseluruhan, terutama ketika koneksi terputus saat sel suatu node roaming berada dalam kondisi lemah dalam jaringan ad hoc. Oleh karena itu, diperlukan suatu metode rute yang mempertimbangkan konsumsi bahan bakar dalam jaringan ad-hoc untuk mempertahankan koneksi internet dan meningkatkan masa pakai jaringan. Keamanan menjadi prioritas utama, dengan berbagai metode keamanan yang ditunjukkan, termasuk otentikasi timbal balik, metode deteksi, verifikasi node, dan pembentukan kepercayaan. Baru-baru ini, berbagai metode navigasi telah dikembangkan untuk memperpanjang umur jalur, sehingga meningkatkan kemajuan jaringan. Penggunaan teknologi multihop menjadi salah satu perkembangan ini. Solusi jaringan bilateral memungkinkan sistem untuk memilih rute optimal dari berbagai opsi dalam operasi perutean reaktif tunggal.



Gambar 2. Waktu Tunda (Delay)

Veeraiah dan Krishna membuat algoritma penjadwalan multi-jalur yang kuat untuk jaringan ad hoc dengan menggunakan optimasi masalah sebagai titik awal. Mereka menggabungkan Fuzzy C-Means (FCM) dan Fuzzy Probabilistic Neural Network (PNN), dua set teknik penghindaran intrusi yang efektif dari node (CH), untuk menangani masalah kapasitas dan perlindungan dalam jaringan ad hoc. Perutean multipath dilanjutkan dengan pendekatan Bird Swarm Optimization Algorithm (BSWOA), yang menggabungkan Bird Swarm Algorithm (BSA) dengan metode optimasi berbasis paus (WOA).

Prasad dan Ravi merekomendasikan penggunaan protokol EA-DRP, yang mengakibatkan total konsumsi energi yang berkurang. Peningkatan penghematan daya dapat diamati sebagai konsekuensi dari revisi dan investigasi saat ini terhadap kebijakan energi yang efisien dalam konteks jaringan ad hoc.

Menurut temuan simulasi, algoritma EA-DRP secara signifikan meningkatkan rata-rata kehilangan daya jaringan. EA-DRP, yang menggunakan energi lebih sedikit, digunakan untuk meningkatkan koneksi jaringan dan menentukan rute perjalanan antara node yang dapat bergerak di jaringan. Meskipun strategi ini dapat memberikan kinerja yang baik dalam hal efisiensi energi, namun memiliki kinerja buruk terhadap berbagai serangan [6].

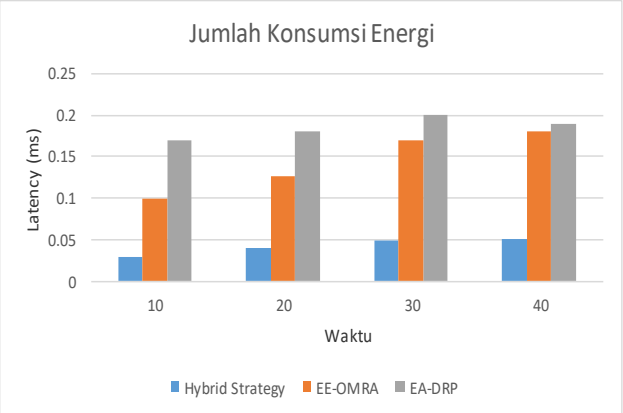
Vijay Kumar dan Saran Anuratha mengusulkan rute Fuel Friendly Goh untuk jaringan seluler ad hoc sebagai variasi dari EEOHRA yang dirancang untuk menggunakan energi lebih sedikit dan memperpanjang umur perangkat. Metode pencarian rute yang diusulkan mempertimbangkan masa pakai perangkat sampai penghitung berkurang saat opsi diaktifkan. Hal ini mengurangi jumlah teknik yang digunakan untuk menemukan rute dan biaya yang dikeluarkan oleh setiap jaringan, keduanya memiliki dampak pada kinerja sistem routing secara keseluruhan.

Taktik ini terbukti tahan terhadap berbagai jenis serangan dan memenuhi standar keamanan. Borkar dan Mahajan memilih solusi yang menerapkan pendekatan heuristik untuk meningkatkan efektivitas energi maksimum dari sistem yang diusulkan. Penyebaran yang berlebihan dari RREQ yang dihasilkan oleh jaringan per periode waktu dicegah dengan pendekatan relay penyaringan [7], yang membuktikan berhasil dalam mengatasi serangan penolakan layanan. Dalam penelitian ini, fokus pada peningkatan keandalan dan ekspansi spektrum untuk protokol AOMDV.

Protokol AOMDV dengan strategi hashing dan metode routing proaktif direkomendasikan oleh Taha et al. menggunakan routing On-Demand Rate Vector (Distance Vector) untuk meningkatkan keamanan terhadap node. Data paket awalnya diangkut dari input ke output menggunakan teknologi perutean. Untuk mengurangi kehilangan paket di seluruh sistem, disarankan penerapan Pencegahan Simpul Egoisme yang Menggunakan Hash (PSNHF) bersama dengan teknik menerima laporan. Selain itu, perutean silang aman berbasis kualitas layanan yang canggih dan infrastruktur enkripsi diperkenalkan untuk meningkatkan efisiensi transmisi data. Studi oleh Tejaswi Kavuru dan Uttej Kohn Nannapaneni melengkapi konsep-konsep ini.

Pendekatan AODV-BR dengan Kontroler Fuzzy yang Dioptimalkan dikembangkan untuk tahap rute gema. Dengan menerapkan metode Wolf Optimizing Adaptive Formation, jalur terbaik dapat diidentifikasi. Rute optimal dari berbagai opsi kemudian dipilih untuk melindungi informasi penting dengan menggunakan pendekatan pengelolaan homomorfik, di mana enkripsi digunakan [8]. Metrik seperti latensi ujung ke ujung, rasio propagasi jaringan, dll. digunakan untuk mengevaluasi kinerja pendekatan yang diusulkan.

Mallikarjuna dan Venkanagouda Chanabasavanagouda, dalam tulisan mereka "Strategi Perutean yang Dapat Diandalkan dan Aman dalam Jaringan Ad-hoc dengan Penginderaan Populasi Berlebih," mengusulkan metode yang bertujuan memaksimalkan kecepatan sambil memperhitungkan penundaan rute dengan akurat. Metode ini memperkirakan jumlah energi yang tersisa dan keandalan tautan dalam teknik ini [2]. Selain itu, metode ini juga mempertimbangkan baik daya transmisi tipe data maupun penerimaannya, sehingga menghitung entropi. Log-likelihood ratio (LET) diperoleh menggunakan faktor dasar, dan kemudian dinilai apakah koneksi tersebut stabil (yaitu, kecepatan dan arah node). Parameter ini digunakan oleh jaringan untuk memilih rute mana yang akan diambil saat mengirimkan datagram antar stasiun.



Gambar 3. Jumlah Energi Konsumsi

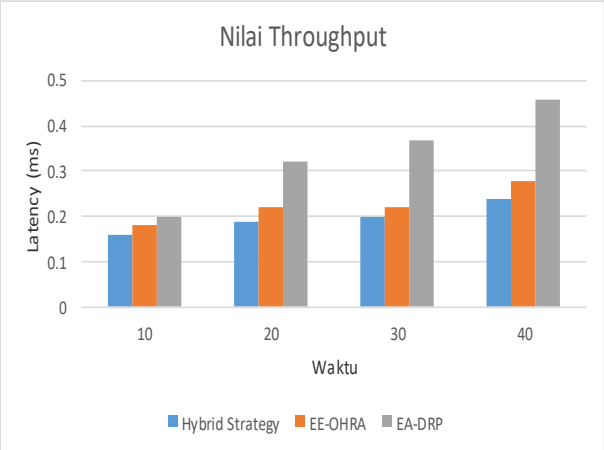
Rajashanthi dan Valarmathi mengklaim bahwa penggunaan tanda tangan untuk memvalidasi bundel paket RREP dalam pemilihan jalur merupakan kombinasi yang dapat diandalkan dari co-relay dan transfer data. Begitu stasiun target menerima bingkai pesan RREP pertama dari klien, semua tandatangan dikonfirmasi, dan pengenal pribadi simpul B menyimpan daftar rute ini di dalam cache. Paket kemudian dikirim ke kedua node tujuan dengan cara yang serupa. Jika biometrik sudah dikonfirmasi, rute tersebut dianggap sah. Sinyal komponen diverifikasi di stasiun pangkalan menggunakan kunci atau hashing. Pengiriman yang aman dapat dimungkinkan tergantung pada tingkat jaminan yang diberikan oleh simpul tunggal. Untuk memilih jalur penemuan rute aman yang optimal, suatu proses diterapkan. Setelah itu, notifikasi dibagi menjadi empat bit, dienkripsi secara lemah, dan ditempatkan melalui prosedur operasi XOR. Setelah surat tersebut telah didekripsi, rahasia akhirnya membantu memulihkannya.

Baik Satyanarayana dan Reddy, yang merupakan subjek utama dari penelitian ini, memfokuskan pada otentikasi dan kerahasiaan data selama pertukaran informasi di seluruh node IoT. Mereka menyarankan strategi mutakhir untuk memperkuat aturan privasi dan memberikan keamanan. Dalam upaya untuk membuat metodologi identifikasi transmisi yang kuat, mereka mempertimbangkan masalah kerusakan asimetris yang bergantung pada teknik pembagian.

Tujuan penelitian ini adalah mengintegrasikan identitas dengan perutean multicast dalam sistem. Selanjutnya, jika satu atau lebih bagian dari sistem tersebut dicegat oleh pihak ketiga, mengambil pesan yang tepat

menjadi suatu tantangan. Rajkumar dan Narsimha [9] mengeksplorasi teknik pengalihan paket dalam Komunikasi Ad Hoc Kendaraan (VANET) dengan menggunakan sejumlah saluran yang berbeda dalam Mobile Ad-hoc Network (jaringan ad hoc). Dengan membagi pengiriman pesan ke dalam beberapa saluran, perutean jalur ganda dapat mendistribusikan pesan di sejumlah jalur, mengatasi potensi kehilangan paket saat melakukan perjalanan melalui salah satu rute.

Untuk mengatasi kesulitan tersebut, Ists (Pemilihan Rute Ekonomis), yang membutuhkan jumlah tertinggi dari spektrum yang dapat digunakan dan jumlah waktu pemancaran yang paling sedikit, digunakan untuk memilih rute alternatif yang paling efisien. Atribut yang diusulkan dalam penelitian ini disajikan dan dievaluasi menggunakan Protocol Suite (NS-2). Parameter baru yang diperkenalkan meningkatkan kecepatan koneksi dengan memilih rute alternatif yang produktif dengan kapasitas yang lebih tinggi.



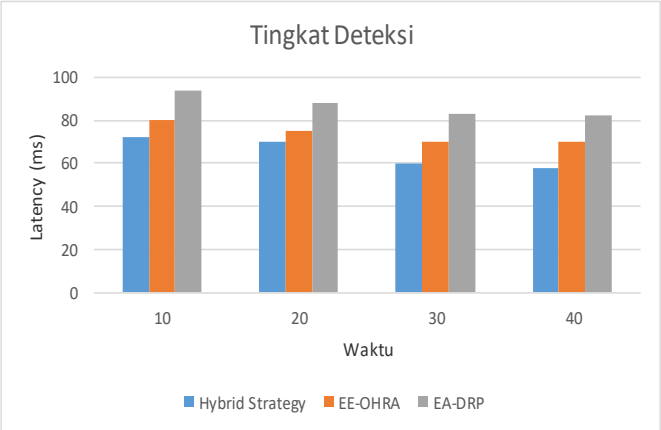
Gambar 4. Nilai Throughput

III. Metode

Dalam perutean yang tepat, tujuannya adalah memastikan bahwa data ditransmisikan secara efektif melalui relay, dengan upaya mengurangi kerugian yang dapat terjadi selama transit pada jaringan seluler ad hoc.

Studi ini juga menghadirkan strategi hibrid yang bertujuan untuk mengurangi disipasi daya saat mendistribusikan listrik dan meningkatkan umur panjang. Beberapa langkah utama termasuk Kategorisasi dan Konstelasi Buram yaitu Pembentukan konstelasi menggunakan pengukuran tegangan eksplisit, implisit, dan harga saat ini. Langkah berikutnya adalah mendefinisikan node yang dirambah dengan menggunakan nilai ambang batas 0,5J yang telah ditentukan. Jika nilai mitra dari node tersebut lebih besar dari persentase kesalahan minimal, itu dianggap sebagai simpul yang berulang., jika tidak, itu juga dianggap sebagai simpul yang diserap.

Dengan langkah-langkah ini, keamanan transfer data dari jaringan awal ke jaringan target dapat dijamin. Jalur yang akurat kemudian dipilih menggunakan pendekatan baru C-SSA (Cat Slapped Solo Algorithm), yang mempertimbangkan fitur-fitur baru yang diinginkan dan juga memperhitungkan kemampuan, kecepatan, dan konektivitas saluran. Cache komposit secara umum mempertimbangkan konsistensi perutean daya yang aman di jaringan ad hoc, seperti yang ditunjukkan dalam Gambar 1.



Gambar 5. Nilai Tingkat Deteksi

IV. Hasil dan Pembahasan

Hasil yang didapatkan terbukti bahwa kategori kinerja dalam iterasi terbaru telah meningkat sehubungan dengan lokasi optimalnya, posisinya di entri sebelumnya, keragaman yang tidak terbatas, atau kecepatannya.

Langkah-langkah dari Cat Jabbed Single Answer (C-SSA) adalah sebagai berikut:

a. Pengaturan Investigasi:

Simulasi menggunakan Ns2 dengan penambahan 100+ port lebih dalam realitas simulasi.

Dalam konteks ini, hasil simulasi dapat direproduksi dengan menggunakan interval waktu sebesar 40 milidetik (mse).

b. Kinerja Metrik

Metrik Kinerja: Pendekatan yang disarankan dibandingkan dengan metode lain yang telah digunakan tergantung pada parameter yang sebanding, termasuk parameter kompetensi, tanpa penyerangan. Kriteria yang terdapat dalam laporan mencakup penundaan, kekuatan, kapasitas, dan akurasi yang lebih baik [10]. Daya peralatan, yang merupakan sisa energi di node setelah berhenti berkomunikasi, harus dinilai maksimum untuk menentukan berapa lama telepon akan bertahan. Sinyal keluaran dari unit ini hanya terkait dengan total data yang dikirim oleh jaringan dalam jangka waktu tertentu, sementara interval mencakup seluruh periode waktu yang dibutuhkan untuk mengirimkan data yang komprehensif ini.

Perbandingan hasil simulasi:

1. **Penundaan (Delay):** Gambar 2 menunjukkan analisis proporsional dengan fokus pada penundaan. Penundaan dari ETA-DRP, Fah, dan protokol routing hibrid yang diusulkan adalah 0,007, 0,004, dan 0,003 msec masing-masing. Dibandingkan dengan dua teknik yang digunakan saat ini, yakni Alokasi Efisien dan EA-DRP, pendekatan routing campuran kepercayaan yang diusulkan memperoleh penundaan rendah sebesar 0,005 milidetik.
2. **Konsumsi Energi:** Gambar 3 menunjukkan perbandingan tingkat metabolisme. Pada 40 detik, perutean Agile, Climate Action EEOHRA, dan perutean campuran emisi tinggi yang diusulkan menggunakan 0,24, 0,22, dan 0,12 m Kilowatt-jam listrik masing-masing. Simulasi penelitian menunjukkan bahwa perutean multicast harmonisasi bahan bakar keyakinan mencapai penggunaan daya rendah sebesar 0,12 m joule dibandingkan dengan dua metode efisiensi tinggi EA-DRP & EE-OHRA.
3. **Throughput:** Gambar 4. Menununjukkan nilai Throughput dari metode Ahn, protokol perutean hibrid yang diusulkan, dan metodologi EA-DRP masing-masing adalah 0,64, 0,45, dan 0.745 GHz. Dibandingkan dengan dua teknik yang sudah ada, yakni Power Plan dan solusi Ahn, algoritma relay ganda yang diusulkan meningkatkan throughput jaringan sebesar 0,75 bps, menurut pengujian.
4. **Tingkat Deteksi:** Gambar 5 menampilkan hasil perbandingan berdasarkan tingkat deteksi. EA-DRP, sirkuit EE-OHRA yang efisien, atau skema perutean hibrid listrik kepercayaan yang diusulkan memiliki tingkat deteksi 80%, 75%, dan 90%, sesuai dengan pendekatannya. Dibandingkan dengan dua strategi saat ini, yakni Pendekatan Efisiensi Energi EE-OHRA dan DRPP Rendah Karbon, router hibridisasi listrik yang direkomendasikan memperoleh tingkat deteksi puncak sebesar 90%.

V. Kesimpulan

Sistem nirkabel telah menarik perhatian yang signifikan dari kalangan akademisi karena potensinya. Meskipun begitu, kualitas intrinsik dari semua sistem tersebut membuatnya rentan terhadap berbagai serangan. Meskipun masih jauh adopsi yang luas karena tantangan energi dan keamanan. Router listrik aman berhasil menangani tantangan ini, mengatasi masalah energi dan keamanan.

Rencana pergerakan efisien dirancang dengan menggunakan perhitungan untuk koloni semut kucing dan semut rangrang yang dioptimalkan. Pada Tahap Satu, CH dipilih dengan menggunakan pendekatan jaringan lunak dan sebagai nilai maksimum untuk kepercayaan pribadi, menengah, dan saat ini. Selain itu, tergantung pada nilai target yang dipilih sebelumnya, node yang melanggar diidentifikasi [11]. CH disiapkan untuk mengirimkan datagram ke drainase karena perutean datagram melibatkan banyak lompatan.

Dalam jaringan ad hoc, teknik optimasi C-SSA (gabungan CSO dan SSA) digunakan untuk memilih langkah-langkah perutean inovatif. Plug-in hibrid difokuskan pada kecepatan, kemampuan, dan koneksi rute secara keseluruhan dengan banyak kecepatan konvergensi yang lebih tinggi.

Metode yang diusulkan menghasilkan rasio puncak paket sebesar 0,99, bandwidth penuh 1,03 bps, biaya minimal 0,12 m kilowatt, dan penundaan yang dapat diabaikan sebesar 0,005 ms [12] dengan jumlah hop. Selain itu, metode ini mencapai peningkatan kemampuan deteksi

sebesar 90%. Dibandingkan dengan teknik saat ini, solusi yang direkomendasikan memberikan hasil yang setara dengan serangan paket yang dipilih.

Penelitian lebih lanjut disarankan fokus pada pemeriksaan kinerja jaringan yang diusulkan dengan lebih banyak tindakan pencegahan keamanan.

REFERENSI

[1] X. Wang, "Network Intrusion Detection Scheme Based on IPSO-SVM Algorithm," *2022 IEEE Asia-Pacific Conf. Image Process. Electron. Comput.*, pp. 1011–1014, 2022, doi: 10.1109/IPEC54454.2022.9777568.

[2] T. Choudhury, K. U. Singh, A. Kumar, G. Kumar, S. Gite, and K. Kotecha, "C-QoS-AOMDV : A cluster based QoS aware multipath routing protocol for MANET using hybrid soft computing techniques," *2023 7th Int. Symp. Multidiscip. Stud. Innov. Technol.*, pp. 1–6, 2023, doi: 10.1109/ISMSIT58785.2023.10304911.

[3] K. Chandravanshi, G. Soni, and D. K. Mishra, "Design and Analysis of an Energy-Efficient Load Balancing and Bandwidth Aware Adaptive Multipath N-Channel Routing Approach in MANET," *IEEE Access*, vol. 10, no. October, pp. 110003–110025, 2022, doi: 10.1109/ACCESS.2022.3213051.

[4] H. E. Kiran, "Dynamic Formation for Unmanned Aerial Vehicles Network," *2019 4th Int. Conf. Comput. Sci. Eng.*, pp. 704–708, doi: 10.1109/UBMK.2019.8907078.

[5] Z. Ding, G. S. Member, L. Shen, and S. Member, "Residual-Energy Aware Modeling and Analysis of Time-Varying Wireless Sensor Networks," vol. 25, no. 6, pp. 2082–2086, 2021, doi: 10.1109/LCOMM.2021.3065062.

[6] M. Farokhzad, A. Majidnia, and D. Nesheli, "A smart and innovative method for multiple routing in wireless sensor networks," *2019 5th Iran. Conf. Signal Process. Intell. Syst.*, no. December, pp. 1–5, 2019.

[7] P. R. Satav, "Review On Single-Path Multi-Path Routing Protocol In Manet : A Study," *2016 Int. Conf. Recent Adv. Innov. Eng.*, pp. 1–7, 2016, doi: 10.1109/ICRAIE.2016.7939514.

[8] M. M. Shawara, A. M. Sarhan, and N. A. Elfishawy, "Distance Vector (EA-AOMDV)," pp. 317–322, 2017.

[9] P. Shakya, V. Sharma, and A. Saroliya, "Enhanced Multipath LEACH Protocol for Increasing Network Life Time and Minimizing Overhead in," *2015 Int. Conf. Commun. Networks*, pp. 148–154, 2015, doi: 10.1109/ICCN.2015.30.

[10] K. A. Darabkh, M. G. Alfawares, S. Althunibat, and A. F. Khalifeh, "A Cross-layer Algorithm for Improving AODV Protocol over Vehicular Ad-hoc Networks," *2019 Int. Conf. Wirel. Commun. Signal Process. Netw.*, pp. 548–551.

[11] A. Taiwo, O. Moses, B. Abigail, W. Bolanle, O. Julius, and B. Musiliu, "e-Prime - Advances in Electrical Engineering , Electronics and Energy Energy Management Model for Mobile Ad hoc Network using Adaptive Information Weight Bat Algorithm," *e-Prime - Adv. Electr. Eng. Electron. Energy*, vol. 5, no. August, p. 100255, 2023, doi: 10.1016/j.prime.2023.100255.

[12] J. Zhang and R. Yan, "Centralized Energy-Efficient Clustering Routing Protocol for Mobile Nodes in Wireless Sensor Networks," *IEEE Commun. Lett.*, vol. 23, no. 7, pp. 1215–1218, 2019, doi: 10.1109/LCOMM.2019.2917193.