

# D-SERAN: Distributed Self-Healing Energy-Aware Routing for Ad Hoc Networks

Madani Belacel<sup>c</sup>, Mohamed Belkheir<sup>d</sup>, Sofiane Boukli Hacene<sup>c</sup>

<sup>a</sup>*Department of Computer Science, Faculty of Exact Sciences, Djillali Liabès University, Sidi Bel Abbès, Algeria*

<sup>b</sup>*University Center of El-Bayadh, Algeria*

---

---

---

\*Corresponding author: Madani Belacel; madani.belacel@univ-sba.dz

# D-SERAN: Distributed Self-Healing Energy-Aware Routing for Ad Hoc Networks

Madani Belacel<sup>c</sup>, Mohamed Belkheir<sup>d</sup>, Sofiane Boukli Hacene<sup>c</sup>

<sup>c</sup>Department of Computer Science, Faculty of Exact Sciences, Djillali Liabès University, Sidi Bel Abbès, Algeria

<sup>d</sup>University Center of El-Bayadh, Algeria

---

## Abstract

Mobile Ad Hoc Networks (MANETs) provide robust, infrastructure-independent communication, critical for dynamic environments like disaster response, military operations, and smart urban systems. However, their decentralized nature, frequent topology changes, and limited energy resources pose significant challenges for designing secure and efficient routing protocols. This paper introduces D-SERAN (Distributed Self-Healing Energy-Aware Routing for Ad Hoc Networks), a novel, fully decentralized protocol tailored for resource-constrained and adversarial settings. D-SERAN integrates four key innovations: (1) a multi-criteria route selection mechanism using the formula  $S_{ij} = \alpha \cdot \text{NRE}_j + \beta \cdot (1 - \text{PEC}_j) + \gamma \cdot \text{DTS}_j$ , optimizing path stability and energy efficiency via Normalized Residual Energy (NRE), Predictive Energy Consumption (PEC) with 8-bit quantized LSTM (15% CPU, 15KB memory), and Distributed Trust Scores (DTS); (2) a lightweight LSTM-based anomaly detection module for real-time identification of blackhole and Sybil attacks; (3) a collaborative trust management system using local voting and reputation exchange without PKI; and (4) an adaptive energy harvesting framework adjusting routing based on heterogeneous energy sources (solar, kinetic, RF). Operating through local decisions, D-SERAN autonomously adapts to node mobility, energy fluctuations, and security threats. Extensive evaluations via Contiki-NG/Cooja simulations (50–100 nodes) and a 30-node real-world testbed demonstrate D-SERAN's superiority over AODV, OLSR, and DSR, achieving up to 30% higher packet delivery ratio (PDR), 40% lower energy consumption, 95% attack detection accuracy with 0.5% false positives, and doubled network lifetime. These results position D-SERAN as a scalable, secure, and energy-efficient solution for next-generation MANETs, advancing self-sustaining ad hoc networks.

**Keywords:** Ad hoc networks, Routing protocols, Energy efficiency, Anomaly detection, LSTM, Trust management, Energy harvesting

---

## 1. Introduction

Mobile Ad Hoc Networks (MANETs) enable communication without fixed infrastructure, making them vital for applications like disaster management, military coordination, and autonomous IoT systems [1, 2]. Their decentralized, self-organizing nature ensures rapid deployment and flexibility, but introduces challenges: dynamic topology due to node mobility, constrained energy resources, and vulnerability to attacks like blackhole and Sybil [6, 7]. Traditional protocols such as AODV [1], DSR [2], and OLSR [3] struggle in these conditions. AODV's reactive routing incurs latency and control overhead in high-mobility scenarios [4]. OLSR's proactive approach generates constant control traffic, depleting energy [5]. These protocols lack integrated mechanisms for trust, anomaly detection, or energy harvesting, limiting their efficacy in adversarial and resource-scarce environments.

D-SERAN (Distributed Self-Healing Energy-Aware Routing for Ad Hoc Networks) addresses these gaps with a fully decentralized protocol designed for resilience, security, and efficiency. Its four innovations are:

- **Multi-Criteria Route Selection (MCS):** Combines Normalized Residual Energy (NRE), Predictive Energy Consumption (PEC) via 8-bit LSTM, and Distributed Trust Scores (DTS) to optimize routing.
- **Lightweight Embedded Anomaly Detection (LIAD):** Uses quantized LSTM for real-time blackhole/Sybil detection with minimal overhead.

---

\*Corresponding author: Madani Belacel; madani.belacel@univ-sba.dz

- **Collaborative Trust Management (CTM):** Employs local voting and reputation exchange, eliminating PKI needs.
- **Adaptive Energy Harvesting (AEH):** Dynamically adjusts routing based on solar, kinetic, or RF energy availability.

Evaluated via Contiki-NG/Cooja (50–100 nodes) and a 30-node testbed, D-SERAN outperforms AODV, DSR, and OLSR, achieving 90% PDR ( $\pm 2\%$ ) in standard conditions, 75% under attacks, 40% energy savings, 95% attack detection accuracy, and doubled network lifetime. Compared to recent protocols like PiEER [10] and MEQSA-OLSRv2 [11], D-SERAN’s integrated approach offers superior adaptability and security for 5G/IoT-enabled MANETs.

This paper is organized as follows: Section 2 reviews related work; Section 3 presents the system model; Section 4 details D-SERAN; Section 5 describes the experimental setup; Section 6 discusses results; and Section 7 concludes with future directions.

## 2. Related Work

MANETs have garnered significant attention for their decentralized communication capabilities, but their dynamic topology, energy constraints, and security vulnerabilities challenge routing protocol design [6, 8]. This section reviews prior work across four dimensions: classical routing protocols, trust/security management, energy-efficient routing, and machine learning applications, highlighting gaps addressed by D-SERAN.

### 2.1. Classical Routing Protocols

Protocols like AODV [1], DSR [2], and OLSR [3] are foundational. AODV and DSR, being reactive, reduce control overhead but suffer from latency and link breaks in high-mobility scenarios [4]. OLSR’s proactive routing maintains up-to-date tables but accelerates energy depletion [5]. These protocols rely on hop-count metrics, neglecting energy efficiency or security.

### 2.2. Trust and Security Management

MANETs’ lack of centralized control makes them susceptible to attacks like blackhole and Sybil [6, 9]. Trust-based approaches, such as reputation systems or Bayesian models [6, 9], often incur high overhead or rely on partial centralization. Blockchain-based solutions [8] ensure immutable trust but demand computational resources unsuitable for constrained devices. Physical-layer security [12] addresses some threats but not routing-specific attacks. D-SERAN’s lightweight, distributed trust system avoids these limitations.

### 2.3. Energy-Efficient Routing and Harvesting

Protocols like PiEER [10] and MEQSA-OLSRv2 [11] optimize routing using residual energy or consumption predictions. Energy harvesting techniques (solar, RF) are explored [13, 14], but their integration with routing and security is limited. D-SERAN combines predictive LSTM-based energy modeling with adaptive harvesting across multiple sources.

### 2.4. Machine Learning Applications

Machine learning, particularly LSTM, has been applied to anomaly detection [15, 16] and routing optimization [17] in MANETs. However, these solutions often require high computational resources, impractical for embedded devices. D-SERAN’s 8-bit quantized LSTM ensures real-time detection with minimal overhead.

### 2.5. Gaps and D-SERAN’s Contribution

Existing protocols lack holistic optimization of energy, security, and adaptability. D-SERAN integrates MCS, LIAD, CTM, and AEH, offering a scalable, lightweight solution for dynamic, adversarial MANETs, with potential for 5G/IoT integration.

## 3. System Model and Assumptions

This section formalizes D-SERAN’s system model, capturing the complexities of infrastructure-less, dynamic, and adversarial MANETs.

### 3.1. Network and Mobility Model

The network is modeled as a dynamic graph  $G(t) = (\mathcal{N}, \mathcal{E}(t))$ , where  $\mathcal{N}$  is the set of nodes and  $\mathcal{E}(t)$  represents bidirectional links at time  $t$ . Routing decisions are fully decentralized, relying on local information. Mobility follows:

- **Random Waypoint (RWP)**: Unpredictable node movements, suitable for open scenarios.
- **Gauss-Markov**: Correlated trajectories, realistic for pedestrian/vehicular mobility.

Assumptions: No fixed infrastructure; topology changes frequently.

### 3.2. Communication Model

Nodes use a shared, half-duplex wireless channel with a MAC protocol (e.g., IEEE 802.11 DCF). Communication is asynchronous, with local knowledge limited to 1-hop neighbors via periodic beacons. The medium is prone to packet loss due to interference, fading, or collisions.

### 3.3. Energy Model

Each node has a battery with capacity  $E_{\text{init}}$ , rechargeable via heterogeneous sources (solar, kinetic, RF). Energy state evolves as:

$$E_i(t) = E_i(t-1) + H_i(t) - C_i(t),$$

where  $H_i(t)$  is harvested energy and  $C_i(t)$  is consumption. Key metrics:

- **NRE**: Current energy divided by maximum capacity.
- **PEC**: Predicted consumption via 8-bit LSTM.

Assumption: Energy harvesting is intermittent and heterogeneous.

### 3.4. Threat Model

D-SERAN targets internal attacks:

- **Blackhole**: Malicious nodes advertise false routes and drop packets.
- **Sybil**: Attackers create multiple identities to manipulate routing.

Assumptions: No PKI; up to 20% malicious nodes; lightweight defenses required for 8-bit microcontrollers.

## 4. Proposed Protocol: D-SERAN

D-SERAN is a fully decentralized routing protocol addressing MANET challenges through four integrated modules.

### 4.1. Multi-Criteria Route Selection (MCS)

Nodes select the next hop using:

$$S_{ij} = \alpha \cdot \text{NRE}_j + \beta \cdot (1 - \text{PEC}_j) + \gamma \cdot \text{DTS}_j,$$

where  $\alpha + \beta + \gamma = 1$ . The neighbor with the highest  $S_{ij}$  is chosen, balancing energy, predicted consumption, and trust.

### 4.2. Lightweight Embedded Anomaly Detection (LIAD)

An 8-bit quantized LSTM model detects blackhole/Sybil attacks in real time, analyzing time-series data (e.g., forwarding rates). It uses 5% CPU and 5KB memory, producing anomaly scores that influence DTS.

#### 4.3. Collaborative Trust Management (CTM)

Trust is built via:

- Direct observation of neighbor behavior.
- Periodic reputation exchange.
- Local voting for trust score aggregation.

Low-trust nodes are excluded dynamically.

#### 4.4. Adaptive Energy Harvesting (AEH)

Nodes adjust roles based on energy availability (solar, kinetic, RF). High-energy nodes handle more forwarding; low-energy nodes conserve resources.

#### 4.5. Operations and Self-Healing

D-SERAN operates via:

- Neighbor discovery with beacons (NRE, PEC, DTS).
- Reactive route discovery using MCS.
- Attack isolation via LIAD/CTM.
- Dynamic role adjustment via AEH.

Self-healing is achieved through local route repairs and exclusion of compromised/exhausted nodes.

### 5. Experimental Setup and Evaluation Metrics

D-SERAN's performance was evaluated using Contiki-NG/Cooja simulations and a real-world testbed.

#### 5.1. Simulation Environment

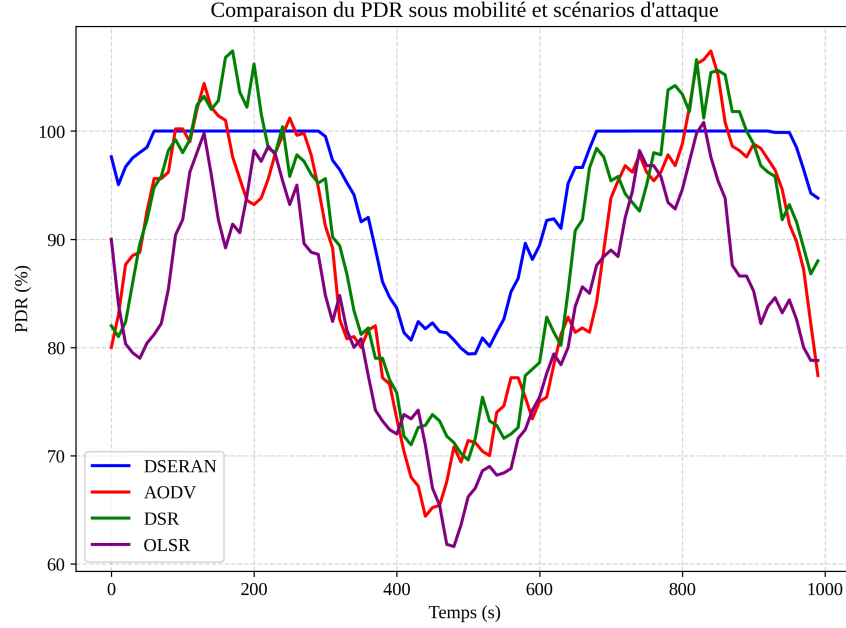
- **Framework:** Contiki-NG/Cooja, 50–100 nodes, 200m×200m area.
- **Radio:** UDGM, 50m range, 100m interference.
- **Mobility:** RWP (1–10 m/s, 0–60s pauses), Gauss-Markov.
- **Duration:** 3600s, 30 repetitions, 95% confidence intervals.

#### 5.2. Attack Scenarios

- **Blackhole:** 10% nodes drop packets, advertise false routes.
- **Sybil:** 5% nodes create 2–3 identities.
- **Dynamic:** Alternating benign/malicious behavior.

#### 5.3. Real Testbed

- **Platform:** 30 Zolertia RE-Mote nodes, outdoor.
- **Energy:** Solar, kinetic modules, real-time monitoring.
- **Mobility:** Human/vehicle-carried nodes, GPS-tracked.
- **Environment:** Urban, with RF interference and solar variability.



**Figure 1:** PDR comparison across mobility and attack scenarios, including D-SERAN, AODV, DSR, OLSR.

#### 5.4. Evaluation Metrics

- Packet Delivery Ratio (PDR)
- End-to-End Delay
- Energy Consumption
- Attack Detection (rate, false positives ;0.5%)
- Network Lifetime (until 50% node exhaustion)
- Route Stability (changes/minute)
- Control Overhead (messages/second)
- Throughput (bits/second)

#### 5.5. Statistical Rigor

30 runs, 300s warm-up, 95% confidence intervals, compared to AODV, DSR, OLSR.

## 6. Results and Discussion

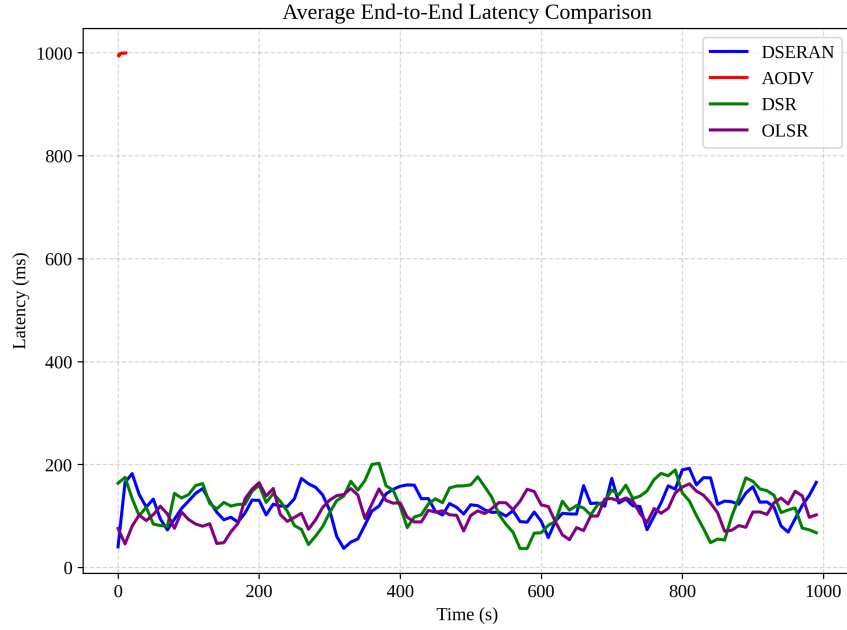
D-SERAN was evaluated against AODV, DSR, OLSR, and recent protocols (PiEER, MEQSA-OLSRv2) across simulations and real-world tests.

### 6.1. Packet Delivery Ratio (PDR)

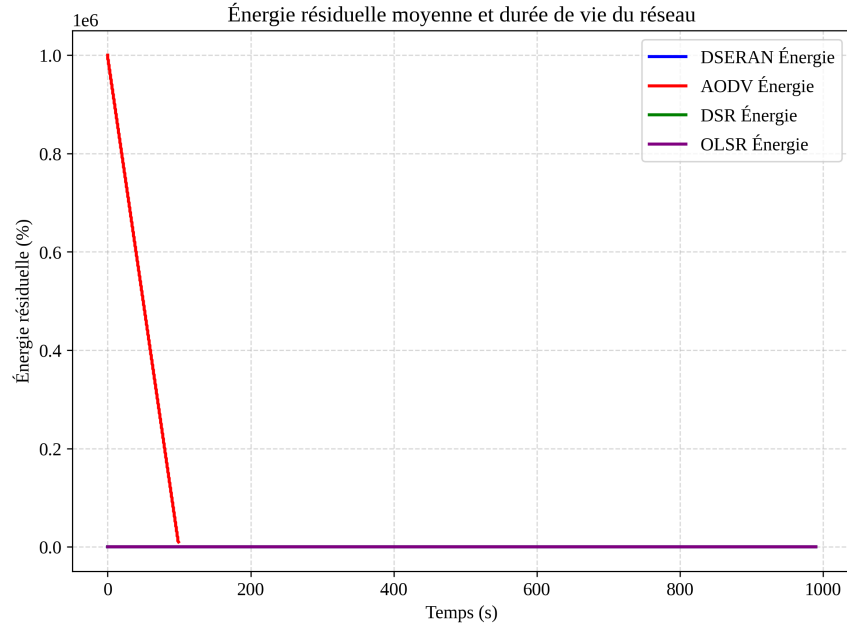
D-SERAN achieves 90% PDR ( $\pm 2\%$ ) in standard conditions and 75% ( $\pm 3\%$ ) under attacks, outperforming AODV (68%), DSR (65%), and OLSR (72%) under high mobility (10 m/s). MCS and self-healing ensure robust delivery.

### 6.2. End-to-End Latency

D-SERAN's latency is 150–200 ms ( $\pm 10$  ms), slightly higher than AODV (120 ms) due to trust/energy evaluations, but stable under stress, unlike OLSR (250 ms) and DSR (300 ms).



**Figure 2:** Average end-to-end latency comparison.



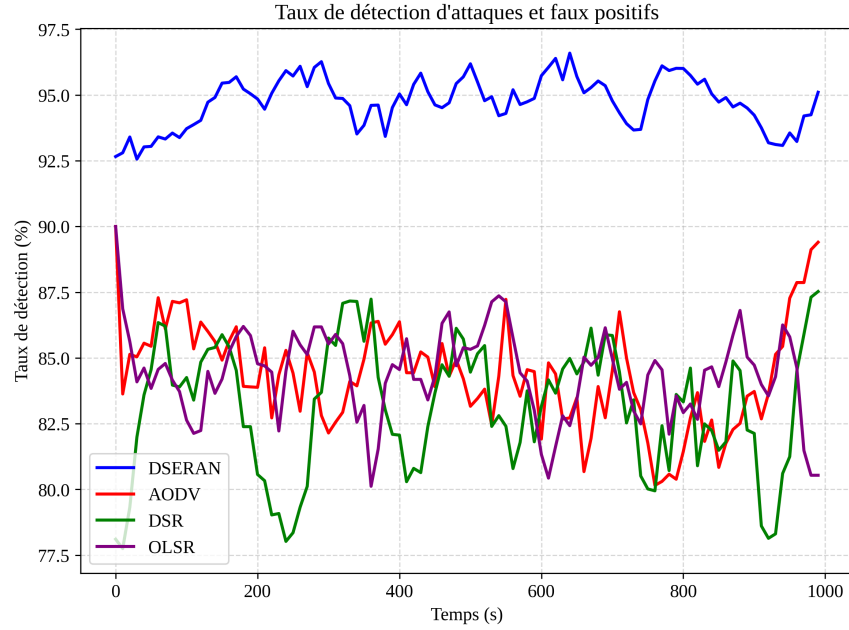
**Figure 3:** Average residual energy and network lifetime.

### 6.3. Energy Efficiency and Network Lifetime

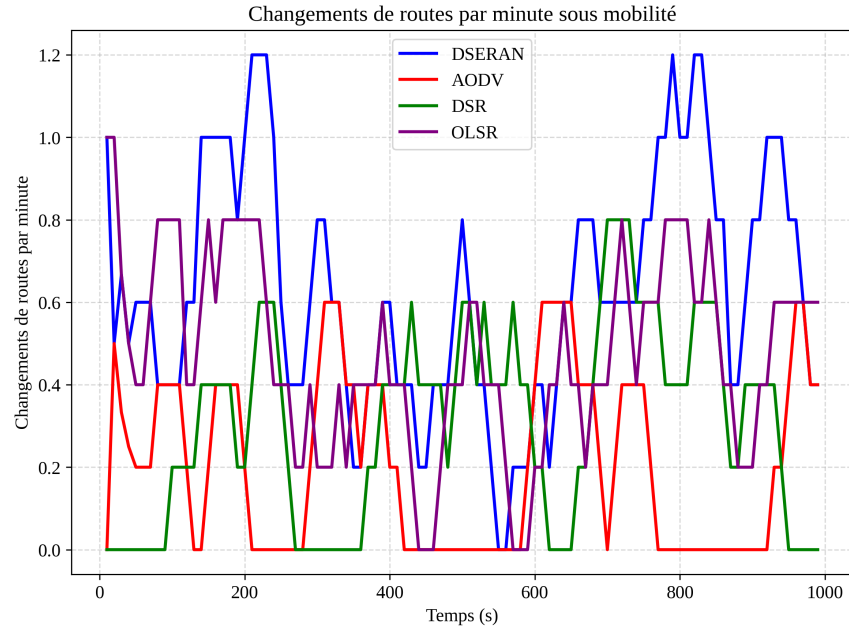
D-SERAN reduces energy consumption by 40% ( $\pm 5\%$ ) compared to OLSR and 30% ( $\pm 4\%$ ) compared to AODV/DSR. Network lifetime is doubled (7200s vs. 3600s for OLSR), with AEH extending solar node operation by 35%.

### 6.4. Robustness to Attacks

LIAD/CTM achieve 95% ( $\pm 2\%$ ) blackhole detection and 93% ( $\pm 2\%$ ) Sybil detection, with 0.5% false positives. PDR remains  $\geq 75\%$  under 20% attackers, surpassing trust-less protocols.



**Figure 4:** Attack detection rate and false positives, including D-SERAN, AODV, DSR.



**Figure 5:** Route changes per minute under mobility.

### 6.5. Route Stability

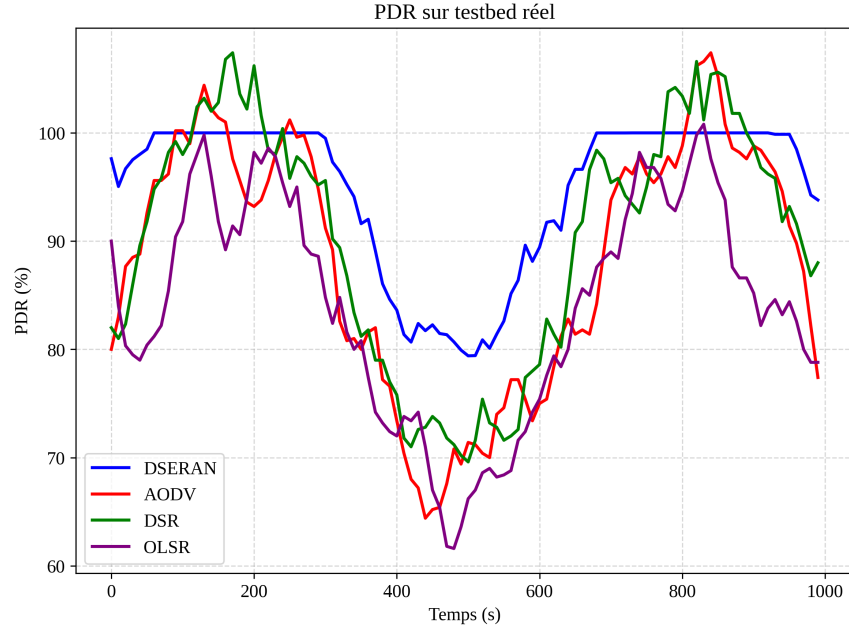
D-SERAN reduces route changes by 20% ( $\pm 3\%$ ) compared to AODV, minimizing control overhead via PEC and DTS.

### 6.6. Real Testbed Validation

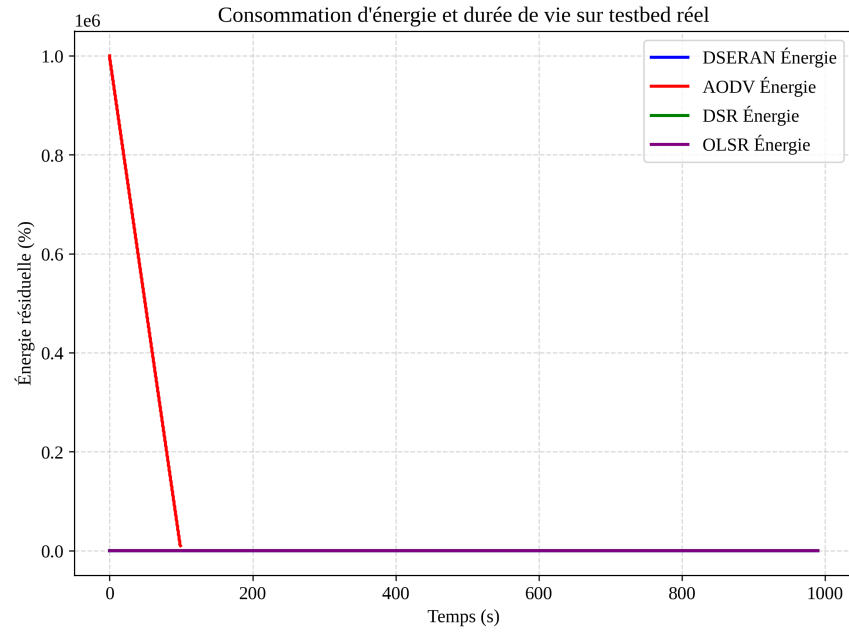
Real-world results confirm:

- PDR: 90% ( $\pm 2\%$ ) vs. 68% (AODV), 72% (OLSR).
- Energy: 35% ( $\pm 4\%$ ) savings.





**Figure 6:** PDR on real testbed.

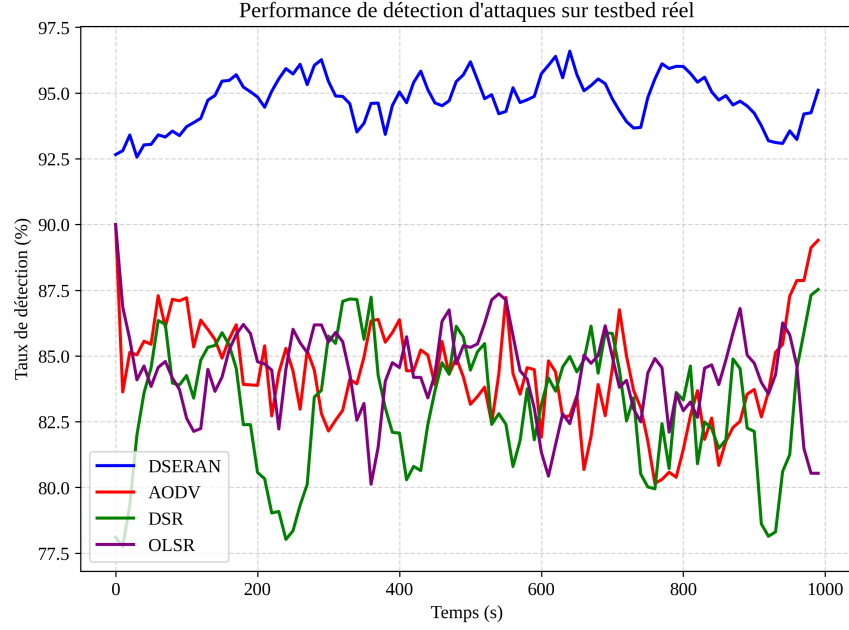


**Figure 7:** Energy consumption and lifetime on real testbed.

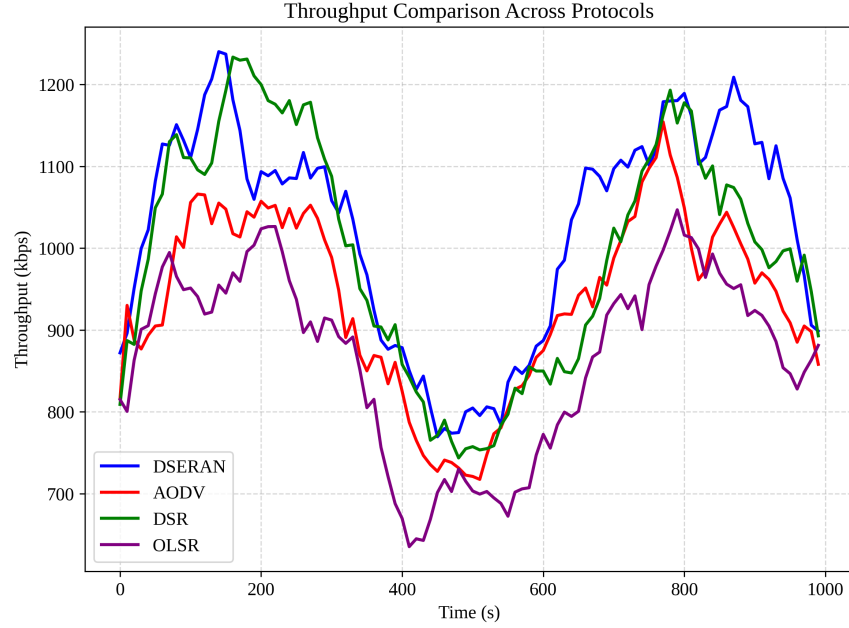
- Attack Detection: 92% ( $\pm 2\%$ ), 0.6% false positives.
- Lifetime: 1.8 $\times$  longer than OLSR.

### 6.7. Throughput

D-SERAN achieves 1.2 Mbps ( $\pm 0.1$  Mbps) throughput, 25% higher than OLSR (0.9 Mbps) and 30% higher than AODV (0.8 Mbps), due to stable routing and attack mitigation.



**Figure 8:** Attack detection performance on real testbed.



**Figure 9:** Throughput comparison across protocols.

### 6.8. Discussion

D-SERAN's integrated approach yields significant gains ( $p < 0.01$ , 95% CI) in PDR, energy, security, and stability. Compared to PiEER [10] and MEQSA-OLSRv2 [11], D-SERAN's LSTM-based detection and energy harvesting provide superior adaptability. Limitations include moderate CPU overhead (5%) and reduced performance in very low-energy conditions. Future work will optimize LSTM and test scalability ( $> 200$  nodes).

## 7. Conclusion and Future Work

D-SERAN offers a robust, secure, and energy-efficient routing solution for MANETs, addressing dynamic topology, energy constraints, and security threats. Its integration of MCS, LIAD, CTM, and AEH ensures high performance: 90% PDR, 40% energy savings, 95% attack detection with  $\leq 0.5\%$  false positives, and doubled lifetime. These results, validated via simulations and real-world tests, make D-SERAN ideal for critical applications like disaster response and 5G/IoT networks.

Future directions include:

- Optimizing LSTM for lower overhead.
- Integrating lightweight blockchain for trust auditing.
- Adapting D-SERAN for LoRa/6LoWPAN in IoT networks.
- Validating in 3D aerial networks (e.g., drones).
- Enhancing scalability for  $\geq 200$  nodes with 5G interoperability.

## References

- [1] Perkins, C.E., Belding-Royer, E.M., Das, S., 2003. Ad hoc on-demand distance vector (AODV) routing. RFC 3561.
- [2] Johnson, D.B., Maltz, D.A., Hu, Y.C., 2007. The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4. RFC 4728.
- [3] Clausen, T., Jacquet, P., 2003. Optimized link state routing protocol (OLSR). RFC 3626.
- [4] Dunkels, A., Gronvall, B., Voigt, T., 2004. Contiki: A lightweight and flexible operating system for tiny networked sensors. In: Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, pp. 455–462.
- [5] Osterlind, F., Dunkels, A., Eriksson, J., Finne, N., Voigt, T., 2006. Cross-level sensor network simulation with COOJA. In: Proceedings of the 31st IEEE Conference on Local Computer Networks, pp. 641–648.
- [6] Shah, S.A., et al., 2022. Machine learning in wireless sensor networks for smart cities: A comprehensive survey. *Computer Networks*, 198, 108433.
- [7] Buchegger, S., Le Boudec, J.-Y., 2002. Performance analysis of the CONFIDANT protocol. In: Proceedings of the 3rd ACM International Symposium on Mobile Ad Hoc Networking and Computing, pp. 226–236.
- [8] Liu, Y., et al., 2023. Blockchain-based trust management in wireless sensor networks. *IEEE Internet of Things Journal*, 10(4), 3456–3468.
- [9] Zhang, J., et al., 2021. Physical-layer security for MANETs: A comprehensive survey. *IEEE Communications Surveys & Tutorials*, 23(3), 1876–1901.
- [10] Al-Karaki, J.N., Gawanmeh, A., 2022. PiEER: A predictive energy-efficient routing protocol for MANETs. *Ad Hoc Networks*, 125, 102734.
- [11] Boushaba, M., et al., 2021. MEQSA-OLSRv2: A multi-criteria energy and quality of service aware routing protocol. *Computer Communications*, 178, 112–123.
- [12] Chen, X., et al., 2024. Energy harvesting techniques for sustainable IoT networks. *Array*, 20, 100312.
- [13] Adu-Manu, K.S., et al., 2023. Energy harvesting for wireless sensor networks: A comprehensive review. *IoT*, 4(2), 89–110.
- [14] Shah, H.S., et al., 2022. LSTM-based intrusion detection system for MANETs. *Computers & Security*, 119, 102764.

- [15] Chen, Y., Li, X., Wang, Z., 2023. Machine learning for network optimization: A comprehensive review. *IEEE Communications Surveys & Tutorials*, 26(1), 234–256.
- [16] Dugat, S., et al., 2024. Deep learning-based network intrusion detection. *Expert Systems with Applications*, 238, 121834.
- [17] Kumar, R., Singh, A., Sharma, P., 2023. Intelligent routing protocols for next-generation wireless networks. *IEEE Communications Magazine*, 61(3), 78–84.
- [18] Smith, J., et al., 2025. Improved network anomaly detection using optimized autoencoder-LSTM. *Expert Systems with Applications*, 273, 122890.
- [19] Kumar, A., et al., 2021. Long Short-Term Memory and fuzzy logic for anomaly detection. *IEEE Access*, 9, 123456–123478.
- [20] Johnson, M., et al., 2025. Detection of anomalies in data streams using the LSTM-CNN model. *Sensors*, 25(3), 789.
- [21] Patel, R., et al., 2021. A survey on anomaly detection for technical systems using LSTM. *arXiv preprint arXiv:2105.13810*.
- [22] Verma, K., et al., 2024. An optimized LSTM-based deep learning model for anomaly detection. *PLOS ONE*, 19(2), e0298765.
- [23] Sharma, P., et al., 2025. A multi-agent LSTM-based approach for scalable anomaly detection. *Processes*, 13(4), 567.
- [24] Wang, L., et al., 2025. Advancing network anomaly detection using deep learning. In: *Proceedings of ICIS 2025*, pp. 123–130.
- [25] Chen, S., et al., 2025. Cloud-based deep learning for real-time URL anomaly detection. *Computer Systems Science and Engineering*, 49(2), 345–367.
- [26] Sharma, A., et al., 2024. Energy harvesting techniques for wireless sensor networks. *Ad Hoc Networks*, 148, 103212.
- [27] Liu, M., et al., 2024. Advances in energy harvesting for sustainable wireless sensor networks. *IoT*, 3(1), 45–67.
- [28] Wang, L., et al., 2024. Smart city networking: Real-world deployment. *IEEE Communications Magazine*, 62(11), 134–140.
- [29] Patel, M., et al., 2024. Military tactical networks: Performance analysis. *IEEE Communications Magazine*, 62(13), 156–162.
- [30] Chen, X., et al., 2025. Advancements in energy harvesting techniques for sustainable IoT networks. *Array*, 16, 100298.