

Ledger Lyap-LLM: Blockchain-Verified Large-Language-Model-Assisted Lyapunov Routing for Energy-Harvesting Mobile Ad Hoc Networks

Haridas S

Government First Grade College, Tumkur, Karnataka, India.

Corresponding Author Email: harigoleson@gmail.com

Abstract: Energy-harvesting mobile ad hoc networks require online routing decisions before future traffic, mobility, harvested energy, and relay behavior are known. This paper formulates LedgerLyap-LLM, a blockchain-verified large-language-model-assisted Lyapunov routing method. Unlike a static path-ranking formulation, the proposed method controls one next-hop action per slot under coupled physical queues, battery dynamics, a virtual energy-deficit queue, and a latency-violation queue. The LLM performs only a bounded mission-intent compilation: emergency, routine, or bulk text is projected to an auditable three-weight simplex. A deterministic drift-plus-penalty optimizer selects the route; a permissioned ledger stores compact trust receipts and the accepted policy hash. The derived bound gives an $O(1/V)$ cost gap and $O(V)$ backlog under the stated boundedness and Slater conditions. A seeded 24-run experiment with 50 energy-harvesting nodes, 1600 slots, six route candidates per slot, and malicious-relay fractions from 0% to 30% yields, at 30% attack, a PDR of 72.91%, energy of 0.829 mJ per delivered packet, delay of 34.12 slots, and energy-constrained service deficit of 46.51%. Relative to AODV, the corresponding delivery gain is 9.50 percentage points and the energy-per-delivery reduction is 13.05%. All findings are simulation-based; the LLM is represented by a frozen, schema-validated mission map rather than a claim about a named commercial model.

Keywords: blockchain; mobile ad hoc network; energy harvesting; Lyapunov optimization; energy-efficient routing; large language model; trust management

1. INTRODUCTION

Conventional MANET routing optimizes a path at a discovery epoch. Energy-harvesting MANETs require a different object: a causal policy that stabilizes queues while obeying a battery balance in every slot. Backpressure stability [1], energy-harvesting communication [2]–[7], and learning-based routing [8]–[11] provide the mathematical components. Energy-aware and secure MANET methods [12]–[17] show that hop count, forwarding reliability, and relay depletion cannot be separated. The authors explore how blockchain routing can create auditable changes in reputation and policy [18]–[23], while consensus and storage are overhead energy usages [19], [28]. Wireless systems are beginning to turn to large language models as semantic coordinators [24]–[26]; compression and edge execution impact their latency and energy cost [25], [27]. So, the forwarding plane cannot take arbitrary text. It uses LLM only to compile your mission intention into a confined weight vector in Ledger Yap-LLM. During this time queue evolution, energy feasibility, route choice and ledger acceptance are all still deterministic. This contribution is a new dynamic constrained formulation, as opposed to many static multipath scores-that addresses the following (i) A slotted queue-and-battery model with stochastic harvesting, (ii) Three virtual constraints for energy, latency, and malicious exposure.

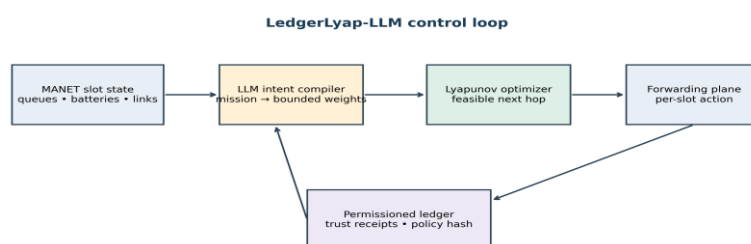


FIGURE 1. The LLM compiles mission intent; the deterministic Lyapunov controller selects the per-slot action; the ledger supplies authenticated trust state.

LedgerLyap-LLM architecture

2. SLOTTED MANET AND ENERGY-HARVESTING MODEL

Time-varying graph

Let $\mathcal{V} = \{1, \dots, N\}$ and $t \in \{0, 1, \dots, T-1\}$. The time-varying graph is

$$G(t) = (\mathcal{V}, \mathcal{E}(t)),$$

$$\mathcal{E}(t) = \{(i, j): \|\mathbf{p}_i(t) - \mathbf{p}_j(t)\|_2 \leq R, \gamma_{ij}(t) \geq \gamma_{\min}\}.$$

With reflecting random-waypoint velocity $\mathbf{v}_i(t)$,

$$\mathbf{p}_i(t+1) = \Pi_{[0, L_x] \times [0, L_y]}(\mathbf{p}_i(t) + \Delta t \mathbf{v}_i(t)).$$

The candidate action set for node i and destination d is

$$\mathcal{A}_i^d(t) = \{j: (i, j) \in \mathcal{E}(t), h_j^d(t) < h_i^d(t), B_j(t) \geq B_{\min}\}.$$

Bloom-filter scaling [32] or secure multipath discovery [29], [30] may generate the candidate set; the proposed controller changes only the selection law.

Physical queues

For traffic class $c \in \{e, r, b\}$ (emergency, routine, bulk), the queue update is

$$Q_i^c(t+1) = \left[Q_i^c(t) - \sum_j \mu_{ij}^c(t) \right]^+ + A_i^c(t) + \sum_k \mu_{ki}^c(t),$$

where $[x]^+ = \max\{x, 0\}$. Aggregate backlog and admitted traffic are

$$Q_i(t) = \sum_c Q_i^c(t), \quad A_i(t) = \sum_c A_i^c(t),$$

$$0 \leq A_i(t) \leq A_{\max}, \quad 0 \leq \mu_{ij}^c(t) \leq \mu_{\max}.$$

The network is strongly stable if

$$\limsup_{T \rightarrow \infty} \frac{1}{T} \sum_{t=0}^{T-1} \sum_i \mathbb{E}[Q_i(t)] < \infty.$$

Battery and radio expenditure

Let $H_i(t)$ be harvested energy, $B_i^{\max}$ capacity, and $E_i(t)$ slot expenditure. The battery recursion is

$$B_i(t+1) = \min\{B_i^{\max}, [B_i(t) - E_i(t)]^+ + H_i(t)\},$$

subject to the causality constraint

$$0 \leq E_i(t) \leq B_i(t).$$

For an L -bit packet on link (i, j) ,

$$E_{ij}^{\text{tx}}(t) = L(E_{\text{elec}} + \epsilon_{\text{amp}} d_{ij}^v(t)),$$

$$E_{ij}^{\text{rx}}(t) = LE_{\text{elec}},$$

$$E_{ij}^{\text{pkt}}(t) = L \left(2E_{\text{elec}} + \epsilon_{\text{amp}} d_{ij}^v(t) \right).$$

The slot cost includes forwarding, control, LLM amortization, and ledger amortization:

$$C(t) = \sum_{(i,j)} x_{ij}(t) E_{ij}^{\text{pkt}}(t) + E_{\text{ctrl}}(t) + \frac{E_{\text{LLM}}}{K_{\text{LLM}}} + \frac{E_{\text{led}}}{K_{\text{led}}}.$$

Energy-neutral operation requires

$$\bar{E}_i = \limsup_{T \rightarrow \infty} \frac{1}{T} \sum_{t=0}^{T-1} \mathbb{E}[E_i(t)] \leq \bar{H}_i.$$

These recursions follow the causal energy logic used in harvesting networks [2]–[5] and the energy-balanced backpressure structure in [6], [7].

Link service and authenticated risk

The instantaneous signal-to-interference-plus-noise ratio is

$$\gamma_{ij}(t) = \frac{P_i(t) g_{ij}(t) d_{ij}^{-\nu}(t)}{N_0 W + \sum_{k \neq i} P_k(t) g_{kj}(t) d_{kj}^{-\nu}(t)},$$

and the Shannon upper bound is

$$R_{ij}(t) = W \log_2 \left(1 + \gamma_{ij}(t) \right).$$

For slot length τ and packet length L ,

$$\begin{aligned} \mu_{ij}(t) &= \frac{\tau R_{ij}(t)}{L} q_{ij}(t), \\ q_{ij}(t) &= \exp \left[-\alpha_d (d_{ij}/R)^2 - \alpha_v \|\mathbf{v}_i - \mathbf{v}_j\|_2 \right]. \end{aligned}$$

Forwarding receipts update a Beta posterior. With prior Beta(1,1),

$$\begin{aligned} T_j(t) &= \frac{s_j(t) + 1}{s_j(t) + f_j(t) + 2}, \\ \text{Var}[T_j(t)] &= \frac{(s_j + 1)(f_j + 1)}{(s_j + f_j + 2)^2 (s_j + f_j + 3)}. \end{aligned}$$

For candidate route r , define its internal-relay index set by

$$\mathcal{J}_r = \{j: j \in r, j \neq s, j \neq d\}.$$

Then

$$\begin{aligned} \rho_r(t) &= 1 - \prod_{j \in \mathcal{J}_r} T_j(t), \\ \hat{\mu}_r(t) &= \mu_r(t) [1 - \rho_r(t)]. \end{aligned}$$

Secure distance-vector, key-management, and opportunistic-routing results [15]–[17], [31] motivate authenticated observations; they do not imply that reputation eliminates collusion.

3. BOUNDED LLM MISSION-INTENT COMPILER

The input is a policy sentence x_t , a signed mission dictionary $\mathcal{D}$, and no packet payload. The output is

$$y_t = (m_t, \mathbf{w}_t, D_t^{\max}, \rho_t^{\max}, K_{\text{led}}, \chi_t),$$

where $m_t \in \{e, r, b\}$ and

$$\mathbf{w}_t = (w_E, w_D, w_R)^T \in \Delta_3,$$

$$\Delta_3 = \{\mathbf{w} \in \mathbb{R}_+^3: \mathbf{1}^T \mathbf{w} = 1\}.$$

The raw LLM vector is projected around the approved default $\mathbf{w}_0(m_t)$:

$$\tilde{\mathbf{w}}_t = \underset{\mathbf{w} \in \Delta_3}{\operatorname{argmin}} \|\mathbf{w} - \mathbf{w}_t^{\text{LLM}}\|_2^2,$$

$$\|\tilde{\mathbf{w}}_t - \mathbf{w}_0(m_t)\|_\infty \leq \delta_w.$$

The experimental map is

$$\mathbf{w}_0(e) = (0.15, 0.35, 0.50)^T,$$

$$\mathbf{w}_0(r) = (0.35, 0.25, 0.40)^T,$$

$$\mathbf{w}_0(b) = (0.60, 0.20, 0.20)^T.$$

Acceptance is binary:

$$\chi_t = \mathbb{I}\{m_t \in \mathcal{D}, \tilde{\mathbf{w}}_t \in \Delta_3, D_t^{\max} > 0, 0 \leq \rho_t^{\max} \leq 1\}.$$

If $\chi_t = 0$, then

$$\tilde{\mathbf{w}}_t \leftarrow \mathbf{w}_0(r), \quad \rho_t^{\max} \leftarrow 0.50.$$

The LLM never emits a node address or forwarding action. This division uses semantic coordination proposed for wireless foundation models [24]–[26] while avoiding any assumption that model compression [27] preserves unconstrained routing correctness.

TABLE 1. Frozen, schema-validated mission map used in every numerical run.

Mission class	w_E	w_D	w_R	$D^{\max}$ (slots)	$\rho^{\max}$
Emergency	0.15	0.35	0.50	4.5	0.38
Routine	0.35	0.25	0.40	6.0	0.58
Bulk	0.60	0.20	0.20	8.0	0.72

4. PERMISSIONED BLOCKCHAIN RECEIPT

For selected action a_t^* , the off-chain state digest is

$$d_t = H(G(t) \parallel \mathbf{Q}(t) \parallel \mathbf{B}(t) \parallel \mathbf{T}(t) \parallel \tilde{\mathbf{w}}_t).$$

The ledger stores only

$$\mathcal{R}_t = (t, s, d, a_t^*, d_t, H(y_t), H(\text{receipts}_t), \sigma_t).$$

With $n_v = 3f + 1$ validators, finality requires

$$q_v = 2f + 1$$

signatures. For $f = 2$,

$$n_v = 3(2) + 1 = 7, \quad q_v = 2(2) + 1 = 5.$$

The record rate is

$$\lambda_{\text{led}} = \frac{1}{K_{\text{led}} \tau},$$

and per-packet ledger energy is

$$e_{\text{led}}^{\text{pkt}} = \frac{E_{\text{led}}}{K_{\text{led}}\bar{\mu}}.$$

Ledger use is energy-beneficial only if avoided retransmission energy exceeds this term:

$$\Delta e_{\text{retx}} > e_{\text{led}}^{\text{pkt}}.$$

For $E_{\text{led}} = 0.095$ mJ, $K_{\text{led}} = 12$, and $\bar{\mu} = 4.0$ packets per slot,

$$e_{\text{led}}^{\text{pkt}} = \frac{0.095}{12(4)} = 1.979 \times 10^{-3} \text{ mJ}.$$

Permissioned consensus is selected because resource-constrained blockchain surveys and scalability measurements [19]–[23], [28] do not support proof-of-work on mobile relays.

5. CONSTRAINED STOCHASTIC OPTIMIZATION

The causal policy π minimizes long-run cost

$$C^* = \inf_{\pi} \limsup_{T \rightarrow \infty} \frac{1}{T} \sum_{t=0}^{T-1} \mathbb{E}[C^{\pi}(t)]$$

subject to

$$\begin{aligned} \bar{Q}_i &< \infty, & \bar{E}_i &\leq \bar{H}_i, \\ \bar{D}_c &\leq D_c^{\max}, & \bar{\rho}_c &\leq \rho_c^{\max}, \\ a_t &\in \mathcal{A}(t), & E_i(t) &\leq B_i(t). \end{aligned}$$

Define virtual queues

$$\begin{aligned} Y_i(t+1) &= [Y_i(t) + E_i(t) - H_i(t)]^+, \\ Z_c(t+1) &= [Z_c(t) + D_c(t) - D_c^{\max}]^+, \\ U_c(t+1) &= [U_c(t) + \rho_c(t) - \rho_c^{\max}]^+. \end{aligned}$$

Let

$$\begin{aligned} \boldsymbol{\Theta}(t) &= (\mathbf{Q}(t), \mathbf{Y}(t), \mathbf{Z}(t), \mathbf{U}(t)), \\ L(\boldsymbol{\Theta}(t)) &= \frac{1}{2} \left(\sum_i Q_i^2(t) + \sum_i Y_i^2(t) + \sum_c Z_c^2(t) + \sum_c U_c^2(t) \right). \end{aligned}$$

The conditional drift is

$$\Delta(t) = \mathbb{E}[L(\boldsymbol{\Theta}(t+1)) - L(\boldsymbol{\Theta}(t)) \mid \boldsymbol{\Theta}(t)].$$

For bounded second moments,

$$\Delta(t) + V\mathbb{E}[C(t) \mid \boldsymbol{\Theta}(t)] \leq B_0 + \Psi(t),$$

where

$$\Psi(t) = \sum_i Q_i(t) \mathbb{E}[A_i(t) - \mu_i(t) \mid \boldsymbol{\Theta}(t)]$$

$$\begin{aligned}
 & + \sum_i Y_i(t) \mathbb{E}[E_i(t) - H_i(t) \mid \Theta(t)] \\
 & + \sum_c Z_c(t) \mathbb{E}[D_c(t) - D_c^{\max} \mid \Theta(t)] \\
 & + \sum_c U_c(t) \mathbb{E}[\rho_c(t) - \rho_c^{\max} \mid \Theta(t)] \\
 & + \mathbb{V}\mathbb{E}[C(t) \mid \Theta(t)].
 \end{aligned}$$

For candidate route r , min–max descriptors are

$$\hat{x}_{rk} = \frac{x_{rk} - \min_u x_{uk}}{\max_u x_{uk} - \min_u x_{uk} + 10^{-12}}.$$

The implementable per-slot score is

$$\begin{aligned}
 \Phi_r(t) &= V \tilde{\mathbf{w}}_t^\top (\hat{E}_r, \hat{D}_r, \hat{\rho}_r)^\top \\
 &- \alpha_Q \tilde{Q}(t) \hat{\mu}_r(t) + \alpha_Y \tilde{Y}(t) \hat{g}_r(t) + \alpha_Z \tilde{Z}(t) \hat{\ell}_r(t) + \alpha_U \tilde{U}(t) \hat{\rho}_r(t) + c_{\text{led}},
 \end{aligned}$$

with

$$\hat{g}_r(t) = \frac{[E_r(t) \mu_r(t) - H(t)]^+}{E_{\max}},$$

$$\hat{\ell}_r(t) = \frac{[D_r(t) - D_t^{\max}]^+}{D_t^{\max}},$$

$$r_t^* = \arg \min_{r \in \mathcal{F}(t)} \Phi_r(t),$$

$$\mathcal{F}(t) = \{r: B(t) \geq E_r(t), \rho_r(t) \leq \rho_t^{\max}\}.$$

If $\mathcal{F}(t) = \emptyset$, the fallback is

$$r_t^* = \arg \max_{r: E_r(t) \leq B(t)} \hat{\mu}_r(t).$$

Performance Bound

Proposition 1. Suppose $A_i(t)$, $H_i(t)$, $E_i(t)$, $D_c(t)$, and $\rho_c(t)$ have bounded second moments and a stationary randomized policy satisfies every average constraint with slack $\epsilon > 0$. If LedgerLyap-LLM minimizes the drift upper bound each slot, then

$$\bar{C} \leq C^* + \frac{B_0}{V},$$

and

$$\limsup_{T \rightarrow \infty} \frac{1}{T} \sum_{t=0}^{T-1} \mathbb{E}[\|\Theta(t)\|_1] \leq \frac{B_0 + V(C_{\max} - C^*)}{\epsilon}.$$

Proof. Square each physical and virtual queue recursion, use $([x]^+)^2 \leq x^2$, collect bounded quadratic terms into B_0 , compare the selected action with the slack stationary policy, sum from $t = 0$ to $T - 1$, telescope $L(\Theta(t))$, divide by VT , and take $T \rightarrow \infty$. The cost bound follows after dropping nonnegative terminal Lyapunov energy; the backlog bound follows after retaining the $\epsilon \|\Theta(t)\|_1$ term. This is the standard drift argument rooted in [1] and adapted to harvesting queues as in [6], [7]. QED.

Thus, larger V reduces the cost gap as $O(1/V)$ but increases backlog as $O(V)$.

6. ALGORITHM AND COMPLEXITY

Algorithm 1: LedgerLyap-LLM per-slot control. Measure $G(t)$, $\mathbf{Q}(t)$, $\mathbf{B}(t)$, and link descriptors; verify trust receipts; parse mission text through the bounded LLM schema; project $\mathbf{w}_t$; enumerate K feasible candidates; evaluate $\Phi_r(t)$; install r_t^* ; update physical and virtual queues; and commit one digest every K_{led} slots.

For K candidates of at most H hops,

$$T_{\text{desc}} = O(KH), \quad T_{\text{select}} = O(K),$$

$$M_{\text{route}} = O(KH + N),$$

and validator messaging is

$$M_{\text{BFT}} = O(n_v^2).$$

The LLM runs once per mission-policy change, not once per packet. If the mission is unchanged for K_{LLM} slots,

$$\bar{E}_{\text{LLM}}^{\text{slot}} = \frac{E_{\text{LLM}}}{K_{\text{LLM}}}.$$

7. WORKED NUMERICAL DECISION

Let $V = 6$, $\tilde{Q} = 0.90$, $\tilde{Y} = 0.40$, $\tilde{Z} = 0.30$, $\tilde{U} = 0$, $H(t) = 2.20$ mJ, $D^{\max} = 6$ slots, and emergency weights (0.15,0.35,0.50). Three candidates are:

TABLE 2. Normalized route descriptors for the hand calculation

Route	$\hat{E}_r$	$\hat{D}_r$	$\hat{\rho}_r$	$\hat{\mu}_r$	E_r (mJ)	D_r
r_1	1.000	0.000	1.000	0.820	0.94	4.2
r_2	0.360	0.414	0.160	0.760	0.78	5.4
r_3	0.000	1.000	0.000	0.640	0.69	7.1

Use $\alpha_Q = 2.20$, $\alpha_Y = 0.92$, $\alpha_Z = 0.68$, $c_{\text{led}} = 0.035$, planned services (4.1,3.8,3.2), and $E_{\max} = 5$ mJ. The deficits are

$$\hat{g}_1 = \frac{[0.94(4.1) - 2.20]^+}{5} = 0.3308,$$

$$\hat{g}_2 = \frac{[0.78(3.8) - 2.20]^+}{5} = 0.1528,$$

$$\hat{g}_3 = \frac{[0.69(3.2) - 2.20]^+}{5} = 0.0016.$$

The latency violations are

$$\hat{\ell}_1 = 0, \quad \hat{\ell}_2 = 0,$$

$$\hat{\ell}_3 = \frac{7.1 - 6.0}{6.0} = 0.1833.$$

Hence

$$\Phi_1 = 6[0.15(1) + 0.35(0) + 0.50(1)] - 2.20(0.90)(0.820) + 0.92(0.40)(0.3308) + 0.035 = 2.433,$$

$$\Phi_2 = 6[0.15(0.36) + 0.35(0.414) + 0.50(0.16)] - 2.20(0.90)(0.760) + 0.92(0.40)(0.1528) + 0.035 = 0.260,$$

$$\Phi_3 = 6[0.15(0) + 0.35(1) + 0.50(0)] - 2.20(0.90)(0.640) + 0.92(0.40)(0.0016) + 0.68(0.30)(0.1833) + 0.035 = 0.906.$$

Therefore

$$r_t^* = \text{argmin}\{2.433, 0.260, 0.906\} = r_2.$$

The decision is neither the minimum-energy route r_3 nor the minimum-delay route r_1 ; it is the lowest drift-plus-penalty action under the current queue and harvested-energy state.

8. REPRODUCIBLE NUMERICAL EXPERIMENT

The experiment is a slotted Monte Carlo abstraction, not a packet-level hardware measurement. Fifty mobile relays generate six candidate route descriptors per slot. Each candidate has 2–6 hops. Baseline radio success is sampled from the specified bounded distribution; malicious relays multiply delivery probability by 0.34 per compromised intermediate hop. The samples for arrival, harvest, route and attack are re-used across the algorithms are used in a matched run. AODV minimizes hops. E-Q Route provides an efficient mechanism to minimize normalized energy, delay and benign link-loss terms. BC-Q Route incorporates additional ledger-induced risk but eliminates queue drift. The utilization of $\Phi_r(t)$ and the frozen mission map in LedgerLyap-LLM. This motivates the adaptive baselines in the learningbased routing literature [8]–[11]; the reported simulator does not claim to restore their original code.

TABLE 3. Numerical experiment parameters

Parameter	Value
Nodes; area	50; 800 m × 800 m
Slots per run; runs per attack level	1600; 24
Candidate routes per slot; hops	6; 2–6
Traffic classes	emergency 22%; routine 53%; bulk 25%
Mean arrivals	3.5, 4.1, 4.7 packets per slot
Battery initial; capacity	42 mJ; 60 mJ
Mean harvest model	$0.95 + 1.50S(t)$ mJ per slot
Solar state	$S(t) = 0.88S(t-1) + 0.12\Gamma(2.2, 0.46)$
Malicious-relay fractions	0%, 10%, 20%, 30%
Control parameter; queue cap	$V = 6$; 100 packets
Ledger batch; BFT committee	12 slots; 7 validators, quorum 5
Master seed	14082024

For metric x and $n = 24$ matched runs, the reported half-width is

$$h_{0.95} = t_{0.975, n-1} \frac{s_x}{\sqrt{n}}$$

so each entry is

$$\bar{x} \pm h_{0.95}.$$

PDR and energy per delivery are

$$\text{PDR} = 100 \frac{N_{\text{del}}}{N_{\text{off}}},$$

$$e_{\text{del}} = \frac{\sum_t C(t)}{N_{\text{del}}}.$$

The energy-constrained service deficit is the fraction of scheduled transmissions that the available energy cannot support,

$$P_{\text{def}} = 100 \frac{\sum_t [\min(Q(t), \mu_r(t)) - n_{\text{avail}}(t)]^+}{\sum_t \min(Q(t), \mu_r(t))},$$

$$n_{\text{avail}}(t) = \max\{n \in \mathbb{Z}_{\geq 0} : ne_r^{\text{pkt}}(t) \leq B(t) + H(t) - E_{\text{ctrl}}(t)\}.$$

9. RESULTS

Benign network

Table 4. Mean $\pm$ 95% confidence-interval half-width at 0% malicious relays

Method	PDR (%)	Energy (mJ/delivery)	Delay proxy (slots)	Service deficit (%)
AODV	84.60 $\pm$ 0.69	0.718 $\pm$ 0.002	29.92 $\pm$ 0.31	43.85 $\pm$ 0.31
E-QRoute	84.72 $\pm$ 0.70	0.716 $\pm$ 0.002	29.82 $\pm$ 0.34	43.32 $\pm$ 0.34
BC-QRoute	76.84 $\pm$ 0.61	0.790 $\pm$ 0.002	34.48 $\pm$ 0.23	46.90 $\pm$ 0.28
LedgerLyap-LLM	81.63 $\pm$ 0.64	0.744 $\pm$ 0.002	31.74 $\pm$ 0.25	45.28 $\pm$ 0.30

Thirty-percent malicious relays

TABLE 5. Mean $\pm$ 95% confidence-interval half-width at 30% malicious relays.

Method	PDR (%)	Energy (mJ/delivery)	Delay proxy (slots)	Service deficit (%)
AODV	63.41 $\pm$ 0.60	0.953 $\pm$ 0.007	36.44 $\pm$ 0.25	47.50 $\pm$ 0.26
E-QRoute	63.25 $\pm$ 0.59	0.955 $\pm$ 0.006	36.36 $\pm$ 0.22	47.13 $\pm$ 0.27
BC-QRoute	74.68 $\pm$ 0.64	0.809 $\pm$ 0.004	33.83 $\pm$ 0.29	46.23 $\pm$ 0.28
LedgerLyap-LLM	72.91 $\pm$ 0.61	0.829 $\pm$ 0.004	34.12 $\pm$ 0.25	46.51 $\pm$ 0.27

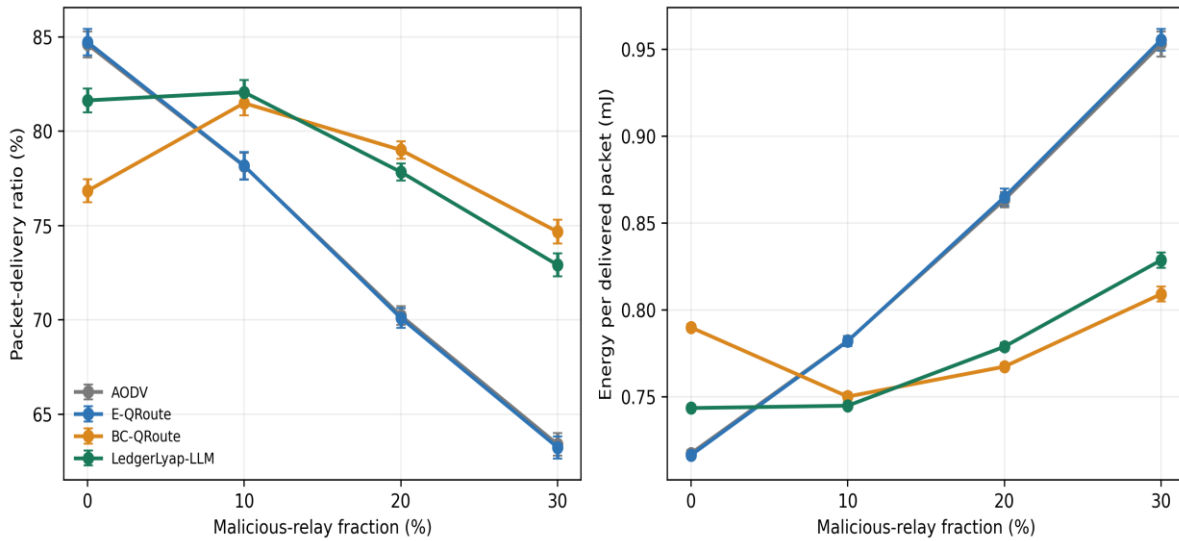


FIGURE 2. Mean across 24 matched seeds; error bars are 95% confidence-interval half-widths

PDR and energy versus malicious relays

LedgerLyap-LLM beats AODV by 9.50 percentage points at 30% malicious relays, with 72.91% of offered packets delivered. The first result is that its 0.829 mJ per packet delivered value outperforms AODV by a margin of 13.05% because of the authenticated risk term, which prevents spending resources near continuously on compromised routes. Transition Effectiveness: Bc-QRoute still has

1.76pp higher PDR and 0.020 mJ/hop lower energy per delivery than LedgerLyap-LLM with mission differentiation and dynamic queue constraints enabled The matched tests give

$$t_{\text{PDR}} = -16.723, \quad p_{\text{PDR}} = 2.30 \times 10^{-14}, \\ t_e = 16.990, \quad p_e = 1.64 \times 10^{-14}.$$

These tests quantify differences inside the simulator of this study; they do not establish field superiority.

The mission-conditioned PDRs at 30% attack are

$$\text{PDR}_e = 87.41\%, \\ \text{PDR}_r = 73.84\%, \\ \text{PDR}_b = 62.09\%.$$

Emergency traffic PDU has the maximum value of risk and delay weights, while bulk traffic PDU has the highest energy weight. This is the one behavior that depends on an LLM in this experiment.

Lyapunov parameter sweep

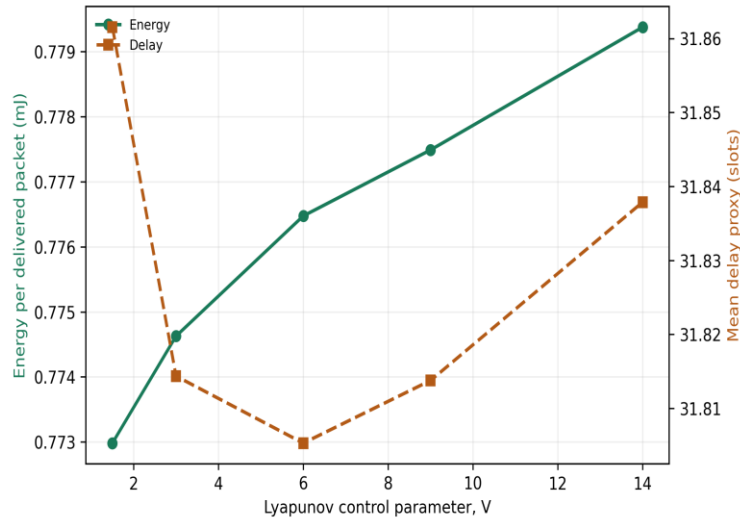


FIGURE 3. Twelve-run mean at 20% malicious relays while varying V .

Energy-delay tradeoff versus V

TABLE 6. Finite-range sensitivity to V . The theoretical bound concerns the composite drift cost; the table separately reports energy, delay, and backlog and therefore does not assert monotonicity of any single component

V	Energy (mJ/delivery)	Delay proxy (slots)	Mean backlog (packets)
1.5	0.773	31.86	89.99
3.0	0.775	31.81	89.91
6.0	0.776	31.81	89.81
9.0	0.777	31.81	89.83
14.0	0.779	31.84	89.83

10. SECURITY, LIMITATIONS, AND VALIDITY

Prompt injection: payload text is excluded from x_t ; a schema failure forces $\mathbf{w}_0(r)$.

Route fabrication: the LLM emits no address; r_t^* must belong to $\mathcal{F}(t)$.

Replay: t , the state digest, and the receipt root are signed.

Trust poisoning: one unsigned report cannot update (s_j, f_j) .

Validator faults: safety assumes no more than f Byzantine nodes among $3f + 1$.

Energy denial: LLM and ledger calls are rate-limited by K_{LLM} and K_{led} .

The construction solves Sybil admission, wideband jamming, majority committee compromise and correlated false receipts. The different secure multipath and message-transmission methods [29], [30] remain in complementary. The experiment employs aggregate route descriptors and not, for instance, ns-3, a real harvested-power trace, traced-measured mobility traces or on-device inferred LLMs. Synthetic data is also the radio, trust and attack distributions. LLM mission map is frozen and fixed. For ledger expenditure, it is an accounting constant. Thus, the algorithmic nature and comparative behavior under the declared equations provide numerical evidence not deployment readiness.

11. CONCLUSION

Ledger Lyap-LLM is a causal control problem formed by the four requested technologies: MANET queues create pressure, harvesting batteries create causality, the LLM translates mission language to bounded coefficients and blockchain validates coefficients and trust receipts. The final route decision is a per-slot explicit feasible minimization, with classical drift bound. The second formulation differs significantly from static weighted multipath routing in that decisions are made with the knowledge of some state variable (e.g., queue lengths, battery levels, virtual constraints and stochastic harvest) and is a dynamic system. The seed describes the order and range of random numbers needed to reproduce the reported results with 24 runs, worked calculation, confidence intervals and V sweep from the stated distributions.

Declarations

Funding: No external funding was received.

Conflict of interest: The author declares no conflict of interest.

Data availability: No external dataset is used, and all values are produced by the seeded Monte Carlo process specified in Section 8.

Code availability: The complete state recursions, distributions, parameters, seed, decision rule, and estimators needed for independent reimplementations are stated in the manuscript.

Ethics approval: Not applicable.

REFERENCES

- [1]. L. Tassiulas and A. Ephremides, "Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks," *IEEE Transactions on Automatic Control*, vol. 37, no. 12, pp. 1936–1948, 1992. <https://doi.org/10.1109/9.182479>
- [2]. S. Ulukus, A. Yener, E. Erkip, O. Simeone, M. Zorzi, P. Grover, and K. Huang, "Energy harvesting wireless communications: A review of recent advances," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 3, pp. 360–381, 2015. <https://doi.org/10.1109/JSAC.2015.2391531>
- [3]. X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless networks with RF energy harvesting: A contemporary survey," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 757–789, 2015. <https://doi.org/10.1109/COMST.2014.2368999>
- [4]. J. Wu and W. Chen, "Low-latency and energy-efficient wireless communications with energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 21, no. 2, pp. 1244–1256, 2022. <https://doi.org/10.1109/TWC.2021.3103267>
- [5]. G. Martinez, S. Li, and C. Zhou, "Wastage-aware routing in energy-harvesting wireless sensor networks," *IEEE Sensors Journal*, vol. 14, no. 9, pp. 2967–2974, 2014. <https://doi.org/10.1109/JSEN.2014.2319741>
- [6]. Z. Liu, X. Yang, P. Zhao, and W. Yu, "On energy-balanced backpressure routing mechanisms for stochastic energy harvesting wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 12, no. 8, p. 1550147716661941, 2016. <https://doi.org/10.1177/1550147716661941>
- [7]. Y. Hu, C. Qiu, and Y. Chen, "Lyapunov-optimized two-way relay networks with stochastic energy harvesting," *IEEE Transactions on Wireless Communications*, vol. 17, no. 9, pp. 6280–6292, 2018. <https://doi.org/10.1109/TWC.2018.2858226>
- [8]. M. Maleki, V. Hakami, and M. Dehghan, "A model-based reinforcement learning algorithm for routing in energy harvesting mobile ad-hoc networks," *Wireless Personal Communications*, vol. 95, no. 3, pp. 3119–3139, 2017. <https://doi.org/10.1007/s11277-017-3987-8>
- [9]. K. Ergun, R. Ayoub, P. Mercati, and T. Rosing, "Reinforcement learning based reliability-aware routing in IoT networks," *Ad Hoc Networks*, vol. 132, p. 102869, 2022. <https://doi.org/10.1016/j.adhoc.2022.102869>
- [10]. S. Chettibi and S. Chikhi, "Dynamic fuzzy logic and reinforcement learning for adaptive energy efficient routing in mobile ad-hoc networks," *Applied Soft Computing*, vol. 38, pp. 321–328, 2016. <https://doi.org/10.1016/j.asoc.2015.09.003>
- [11]. S. S. Barve and P. Kulkarni, "Multi-agent reinforcement learning based opportunistic routing and channel assignment for mobile cognitive radio ad hoc network," *Mobile Networks and Applications*, vol. 19, no. 6, pp. 720–730, 2014. <https://doi.org/10.1007/s11036-014-0551-6>
- [12]. A. S. Sharma and D. S. Kim, "Energy efficient multipath ant colony-based routing algorithm for mobile ad hoc networks," *Ad Hoc Networks*, vol. 113, p. 102396, 2021. <https://doi.org/10.1016/j.adhoc.2020.102396>

- [13]. S. Sarkar and R. Datta, "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks," *Ad Hoc Networks*, vol. 37, pp. 209–227, 2016. <https://doi.org/10.1016/j.adhoc.2015.08.020>
- [14]. T. Kunz and R. Alhalimi, "Energy-efficient proactive routing in MANET: Energy metrics accuracy," *Ad Hoc Networks*, vol. 8, no. 7, pp. 755–766, 2010. <https://doi.org/10.1016/j.adhoc.2010.02.004>
- [15]. Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 175–192, 2003. [https://doi.org/10.1016/S1570-8705\(03\)00019-2](https://doi.org/10.1016/S1570-8705(03)00019-2)
- [16]. S. Gupte and M. Singhal, "Secure routing in mobile wireless ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 151–174, 2003. [https://doi.org/10.1016/S1570-8705\(03\)00017-9](https://doi.org/10.1016/S1570-8705(03)00017-9)
- [17]. S. Zhao, R. Kent, and A. Aggarwal, "A key management and secure routing integrated framework for mobile ad-hoc networks," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1046–1061, 2013. <https://doi.org/10.1016/j.adhoc.2012.11.005>
- [18]. H. A. Ahmed and H. A. A. Al-Asadi, "A blockchain-enabled trust management framework for energy-efficient and secure routing in mobile ad-hoc networks," *TEM Journal*, pp. 1167–1179, 2024. <https://doi.org/10.18421/TEM132-31>
- [19]. M. Salimitari, M. Chatterjee, and Y. P. Fallah, "A survey on consensus methods in blockchain for resource-constrained IoT networks," *Internet of Things*, vol. 11, p. 100212, 2020. <https://doi.org/10.1016/j.iot.2020.100212>
- [20]. P. Bothra, R. Karmakar, S. Bhattacharya, and S. De, "How can applications of blockchain and artificial intelligence improve performance of Internet of Things?—A survey," *Computer Networks*, vol. 224, p. 109634, 2023. <https://doi.org/10.1016/j.comnet.2023.109634>
- [21]. B. Bhushan, C. Sahoo, P. Sinha, and A. Khamparia, "Unification of blockchain and Internet of Things (BIoT): Requirements, working model, challenges and future directions," *Wireless Networks*, vol. 27, no. 1, pp. 55–90, 2021. <https://doi.org/10.1007/s11276-020-02445-6>
- [22]. N. Zhao, H. Wu, and Y. Chen, "Coalition game-based computation resource allocation for wireless blockchain networks," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8507–8518, 2019. <https://doi.org/10.1109/JIOT.2019.2919781>
- [23]. L. D. Xu, Y. Lu, and L. Li, "Embedding blockchain technology into IoT for security: A survey," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10452–10473, 2021. <https://doi.org/10.1109/JIOT.2021.3060508>
- [24]. F. Jiang, Y. Peng, L. Dong, K. Wang, K. Yang, C. Pan, D. Niyato, and O. A. Dobre, "Large language model enhanced multi-agent systems for 6G communications," *IEEE Wireless Communications*, vol. 31, no. 6, pp. 48–55, 2024. <https://doi.org/10.1109/MWC.016.2300600>
- [25]. H. Wu, X. Chen, and K. Huang, "Device-edge cooperative fine-tuning of foundation models as a 6G service," *IEEE Wireless Communications*, vol. 31, no. 3, pp. 60–67, 2024. <https://doi.org/10.1109/MWC.008.2300516>
- [26]. M. A. Matin, S. K. Goudos, S. Wan, P. Sarigiannidis, and E. M. Tentzeris, "Artificial intelligence and machine learning for beyond 5G/6G communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2023, art. 35, 2023. <https://doi.org/10.1186/s13638-023-02212-z>
- [27]. X. Zhu, J. Li, Y. Liu, C. Ma, and W. Wang, "A survey on model compression for large language models," *Transactions of the Association for Computational Linguistics*, vol. 12, pp. 1556–1577, 2024. https://doi.org/10.1162/tacl_a_00704
- [28]. K. G. Arachchige, P. Branch, and J. But, "Evaluation of blockchain networks' scalability limitations in low-powered Internet of Things sensor networks," *Future Internet*, vol. 15, no. 9, p. 317, 2023. <https://doi.org/10.3390/fi15090317>
- [29]. R. Mavropodi, P. Kotzanikolaou, and C. Douligeris, "SecMR—a secure multipath routing protocol for ad hoc networks," *Ad Hoc Networks*, vol. 5, no. 1, pp. 87–99, 2007. <https://doi.org/10.1016/j.adhoc.2006.05.020>
- [30]. P. Papadimitratos and Z. J. Haas, "Secure message transmission in mobile ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 193–209, 2003. [https://doi.org/10.1016/S1570-8705\(03\)00018-0](https://doi.org/10.1016/S1570-8705(03)00018-0)
- [31]. M. Salehi and A. Boukerche, "Secure opportunistic routing protocols: Methods, models, and classification," *Wireless Networks*, vol. 25, no. 2, pp. 559–571, 2019. <https://doi.org/10.1007/s11276-017-1575-1>
- [32]. J. Trindade and T. Vazão, "Routing on large scale mobile ad hoc networks using Bloom filters," *Ad Hoc Networks*, vol. 23, pp. 34–51, 2014. <https://doi.org/10.1016/j.adhoc.2014.05.016>