Int. j. inf. tecnol. (October 2024) 16(7):4299–4307
https://doi.org/10.1007/s41870-024-01975-y

ORIGINAL RESEARCH

Link reliable on-demand distance vector routing for mobile ad hoc networks

Periyasamy Pitchaipillai[1]

Received: 20 February 2024 / Accepted: 29 May 2024 / Published online: 14 June 2024

Abstract An established infrastructure or centralised control system is not necessary for communication between nodes, or mobile devices, in a mobile ad hoc network, or MANET. To adhere to the quality of service (QoS) standards, Unipath routing protocols find a single dedicated route between a pair of solicited source and destination within the network. In this study, a modified version of the popular ad hoc on-demand distance vector (AODV) called the link reliable on-demand distance vector (LRODV) is proposed. The AODV uses the traditional routing measure hop count to determine the shortest path between a source and destination pair, but this does not ensure link dependability. The LRODV uses an enhanced cumulative expected transmission count (enh-CETX) to select a link trustworthy route between a source and destination pair, preventing link failures and route breaks in highly dynamic ad hoc networks. In terms of quality of service (QoS) metrics, the performance of the LRODV protocol using NS 2.35 with different network flows under the random way-point mobility model is compared with that of the AODV routing protocol. The LRODV reduces 4.822741% of routing overhead, 2.938256% of packet loss ratio, 7.429350% of normalised routing overhead, and 0.609278% of energy usage as network traffic increase. In comparison to the AODV routing protocol, it boosts the throughput by 2.741449% and also packet delivery ratio by 2.938256%.

Keywords MANET · AODV · QoS · CBR · Routing metrics · Random waypoint mobility

1 Introduction

A mobile ad hoc network (MANET) [1, 2] is a decentralized type of wireless network that is characterized by the absence of any pre-established infrastructure or centralized administration. In a MANET, mobile nodes communicate with each other directly or through intermediate nodes, forming a dynamic and self-configuring network. This unique feature allows MANETs to be highly flexible and adaptable, making them suitable for various scenarios where traditional infrastructure-based networks may be impractical or unavailable. The characteristics such as Infrastructure-less configuration, dynamic topology, security challenges and resource constraints make MANETs suitable for situations where the deployment of a static infrastructure is challenging in military operations, emergency responses, civilian and certain wireless sensor network applications.

MANETs [1, 2] are used in a wide range of situations, such as wireless sensor networks for environmental monitoring, disaster recovery operations, collaborative work environments, and military communication in dynamic battlefield circumstances. Although MANETs are quite flexible, they still have to deal with concerns like scalability, security in the absence of a centralised authority, and creating efficient routing protocols.

Routing in MANETs is a complex task due to their dynamic nature, requiring specialized protocols like Ad hoc on-demand distance vector (AODV) or dynamic source routing (DSR). Security is also a concern in MANETs, as their open and dynamic nature makes them susceptible to various threats. Encryption and authentication mechanisms are crucial to safeguard against potential attacks. Researchers and engineers continually work on improving the robustness and efficiency of MANETs to meet the demands of diverse

---

✉ Periyasamy Pitchaipillai
pereee@yahoo.com

[1] St. Joseph's University, Bangalore, Karnataka, India

applications. Literature review on ad hoc on-demand distance vector (AODV) is shown in Table 1.

The rest of the paper is organized as follows: The popular unipath routing protocol: In Sect. 2, a brief discussion of ad hoc on-demand distance vector (AODV) is provided. Comparably, Sect. 3 presents an illustration of the suggested protocol; Sect. 4 presents the simulation and experimental results; and Sect. 5 concludes with a discussion on future study.

2 Ad hoc on-demand distance vector (AODV)

The loop-free on-demand or reactive routing protocol known as ad hoc on-demand distance vector (AODV) [9] combines the capabilities of dynamic source routing (DSR) [10, 11] and destination-sequenced distance vector (DSDV) [12] to tolerate a variety of network behaviours, including node mobility, packet losses, and connection failures. The efficiency of AODV is well established in dynamic and resource-constrained contexts, where node mobility can cause frequent changes in the network's architecture. At every node, AODV maintains a routing table. The fields that must be present in a destination's routing table entry are a sequence number, a hop count, and the next hop node. All packets intended for the destination are received by the next hop node. The sequence number serves as a time-stamp and gauges how recent a route is. The hop count indicates the current distance to the destination node.

When a node i receives an RREQ or RREP, it updates its hop count and next hop for a destination d if its sequence number is less than or equal to the sequence number of RREQ or RREP of node j, or if its sequence number is equal to the sequence number of RREQ or RREP of node j and its hop count is greater than the hop count of RREQ or RREP of node j. The above said rules for AODV route update are shown in Algorithm 1.

Algorithm 1 Route update rules of AODV protocol [9]

```
if ($seqnum_i^d < seqnum_j^d$) or (($seqnum_i^d = seqnum_j^d$) and
($hopcount_i^d > hopcount_j^d$)) then
    $seqnum_i^d := seqnum_j^d$
    $hopcount_i^d := hopcount_j^d + 1$
    $nexthop_i^d := j$
end if
```

Key features of AODV are: (i) *On-demand routing*—AODV creates routes only when needed, operating on an as-needed basis. Because of the reduction in overhead

Table 1 Literature review on ad hoc on-demand distance vector (AODV)

Routing metrics	Description
Round trip time (RTT) [3]	By calculating round trip time (RTT) and processing time the malicious nodes forming wormhole attack has been identified [3] but this method does not ensure link reliability
Ramadge wonham (RW) [4]	The Ramadge Wonham (RW) [4] network with a parametric number of nodes is used to define the discrete event systems (DES) in which the Ad-hoc on Demand Distance vector (AODV) routing protocol is implemented whereby the author outlined the following two rules: The first rule ensures the hierarchy of the routing channels and the requests from the nodes. First-level security over query replies is provided by the second rule. Still, there is no assurance that the connections amongst nodes are trustworthy despite this effort
A* and Floyd-algorithm Warshall's Integrated Approach [5]	By employing A* and Floyd-algorithm Warshall's Integrated Approach, the primary objectives of this study are to enhance security in the use of the AODV protocol by identifying the face of one or more black hole assaults [5]. However, this does not ensure the dependability of the link either
Analytic hierarchy process (AHP) and entropy weight method (EWM) Integrated Approach [6]	While reducing average end-to-end latency and energy consumption, the AHP and EWM integrated approach [6] also addresses the significance of energy in applications; nevertheless, link stability is not guaranteed by this study
Dynamic threshold value [7]	In order to protect against black-hole attacks, AODV proposed a dynamic threshold value [7] for the security aspect of MANETs. However, link stability is not guaranteed
A trust based secure and energy aware (T-SEA) routing protocol [8]	Although connection stability is not guaranteed, a trust-based secure and energy aware (T-SEA) [8] routing protocol was developed for the identification and isolation of black/gray hole nodes in mobile ad hoc networks (MANETs)

brought about by the constant updating of routing data, AODV is especially well-suited to situations where energy and bandwidth conservation are vital. (ii) *Route discovery*—A route discovery procedure is started by a source node that wishes to interact with a destination node but does not yet have a valid route. A Route Request (RREQ) packet is broadcast to its neighbors during this process, and these neighbors forward the request until it reaches the destination or a node that has discovered a new route there. (iii) *Route maintenance*—AODV monitors the status of active routes. If a link or node failure occurs, a Route Error (RERR) message is generated and propagated through the network, informing affected nodes to invalidate the broken route. This triggers a new route discovery if needed. (iv) *Loop avoidance*—Routing loops are a prevalent problem in dynamic networks, and AODV has ways to prevent them. Every route has a sequence number assigned to it, which aids nodes in differentiating between outdated and updated routing data. This guarantees that the routing table entries are current and helps to eliminate loops. (v) *Optimized route*—Finding the best path to the destination is the goal of AODV. The routing table's sequence numbers and hop counts allow it to make well-informed decisions about which data transmission method is most dependable and effective.

Advantages of AODV are: (i) *Low overhead*—AODV minimizes control packet overhead by initiating the route discovery process when needed. This leads to efficient use of network resources and reduces congestion. (ii) *Adaptability to dynamic environments*—AODV is well-suited for MANETs due to its ability to adapt to dynamic network topologies caused by node mobility. The on-demand nature of the protocol ensures that routes are only established when necessary, accommodating changes in the network structure. (iii) *Quick Route Establishment*—AODV is known for its relatively quick route establishment process. This is crucial in scenarios where communication needs to be established promptly, such as in military operations or emergency response situations.

3 Proposed protocol: link reliable on-demand distance vector (LRODV)

Communication nodes are susceptible to connection failures and route breakdowns because AODV routing chooses a route between any source and destination pair based on the least possible hop count, which does not ensure end-to-end reliable data transmission. A novel node disjoint routing protocol called Link Reliable On-demand Distance Vector (LRODV) protocol is introduced as a remedy for these problems by extending AODV [9].

3.1 Routing metrics

Routing metrics are the measurements that are used to determine the best route, out of all the options. It falls into two categories: (i) node-based routing metrics, which select the best feasible path based on available information from participating nodes, such as energy and hop count; and (ii) link-based routing metrics, which select the best feasible path based on available information from participating links, such as throughput and reliability.

Every routing protocol measures link stability by default using link expiration time (LET). When a link between nodes are active (its LET is not expired) but outside of the transmission range, it has failed to send data. The scope of our protocol is to dynamically measure enhanced CETX using PROBE Packets in order to guarantee connection stability.

3.2 General Procedure

The suggested protocol is an improved variant of AODV that uses the enhanced Cumulative Expected Transmission Count (enh-CETX) to choose a link trustworthy route between a source and destination pair. This protocol introduces a new received signal strength indicator (RSSI) called PROBE Packet along with RREQ/RREP Packets in order to measure the trustworthy link between nodes. This PROBE Message Format is illustrated in Table 4.

The following is the general procedure of LRODV protocol:

1. Determining enhanced expected transmission count (enh-ETX)
2. Determining enhanced cumulative expected transmission count (enh-CETX)
3. Route selection based on enh-CETX

3.2.1 *Determining enhanced expected transmission count (enh-ETX)*

The number of PROBE packets sent over a period of time known as the enhanced expected transmission count (enh-ETX) is used to assess the quality of a link between participating nodes in the path.

The LRODV protocol calculates $mPRR_{forward(i,j)}$, $mPRR_{backward(i,j)}$, and $enh\text{-}ETX_{link(i,j)}$ during route discovery phase as follows:

$$mPRR_{forward(i,j)} = \frac{Number\ of\ PROBE\ messages\ i\ received\ from\ j}{w\ seconds} \tag{1}$$

The number of PROBE messages generated from the sender j to the receiver i over a given amount of time, say w seconds, is known as the modified Packet Reception Rate, or $mPRR_{forward(i,j)}$, of uplink quality from the sender to the receiver.

$$mPRR_{backward(i,j)} = \frac{Number\ of\ PROBE\ messages\ j\ received\ from\ i}{w\ seconds} \quad (2)$$

The number of PROBE messages generated from sender i to receiver j over a given amount of time, say w seconds, is known as the modified Packet Reception Rate, or $mPRR_{backward(i,j)}$, of downlink quality from the sender to the receiver.

3.2.2 Determining enhanced cumulative expected transmission count (enh-CETX)

Table 3 shows the enhanced Cumulative Expected Transmission Count (enh-CETX), a new field added to each RREQ and RREP in the LRODV protocol. When both $mPRR_{forward(i,j)}$ and $mPRR_{backward(i,j)}$ are 1 and the link between i and j is perfect, so the $enh\text{-}ETX_{link(i,j)}$ is 1. The summation of the enh-ETX values of all participating links in the node-disjoint path is the enh-CETX value of a path from a source node S to a destination node D. This value is computed as follows after determining the enh-ETX of links in a wireless network:

$$enh\text{-}ETX_{link(i,j)} = \frac{1}{mPRR_{forward(i,j)} * mPRR_{backward(i,j)}} \quad (3)$$

Both the downlink quality ($mPRR_{backward(i,j)}$) from the receiver to the sender and the uplink quality ($mPRR_{forward(i,j)}$) from the sender to the receiver are used to determine the value of $enh\text{-}ETX_{link(i,j)}$.

$$enh\text{-}CETX_{path(S,D)} = \sum_{link(i,j)\in path(S,D)} enh\text{-}ETX_{link(i,j)} \quad (4)$$

Where path(S, D) is a set of successive links in the path from node S to D such as: path(S, D) = $\{(S,I_1),(I_1,I_2),\dots,(I_{k-1},I_k),(I_k,D)\}$.

3.2.3 Route selection based on enh-CETX

The enhanced ETX value of each link that an RREQ or RREP has travelled is added to each RREQ and RREP of the LRODV protocol. This field is known as enh-CETX, and it is displayed in Table 3. Table 2 presents the structure of the routing table entries for the AODV and LRODV routing protocols. Table 5 displays the notations and their descriptions that are used in this paper.

Table 2 Structure of routing table entries of AODV and LRODV routing protocols

AODV	LRODV
destination_address	destination_address
sequence_number	sequence_number
hopcount	**enh-cetx**
nexthop	nexthop
expiration_timeout	expiration_timeout

Table 3 Extended RREQ/RREP message format

Source Address	Destination Address	Sequence Number	Hop Count	enh-CETX	Expire

Table 4 PROBE message format

Source Address	Number of Neighbours	Neighbours Addresses	Number of Probes	Expire

Table 5 Notations and their descriptions

Notation	Description
$enh\text{-}ETX_{link(i,j)}$	Enhanced ETX value of link i and j
$enh\text{-}CETX_{path(S,D)}$	Enhanced Path ETX, called as enh-CETX
$mPRR_{forward(i,j)}$	Modified forward packet reception Rate of a link at node i
$mPRR_{backward(i,j)}$	Modified backward packet reception Rate of a link at node j
i,j	Intermediate nodes
S,s	Source node
D,d	Destination node

Similar to the AODV routing protocol, a node in LRODV instantly rebroadcasts an RREQ packet upon receiving it for the first time. The enh-CETX of RREQ/RREP is initialised to 0 when a source S floods RREQ to a destination D or a destination D sends back RREP to a source S. The intermediate nodes determine the enh-ETX value in terms of the quantity of PROBE packets sent across the ends of the link upon receiving the RREQs or RREPs, and Algorithm 2 is used to update the enh-CETX on a regular basis.

Algorithm 2 Route update rules of LRODV protocol

```
if $(seqnum_i^d < seqnum_j^d)$ or $((seqnum_i^d = seqnum_j^d)$ and
$(enh\text{-}cetx_i^d > enh\text{-}cetx_j^d))$ then
    $seqnum_i^d := seqnum_j^d$
    $enh\text{-}cetx_i^d := enh\text{-}cetx_j^d$
    $nexthop_i^d := j$
end if
```

As shown in Algorithm 2, a node i uses LRODV route update rules to set up both forward and reverse routes whenever it gets a route advertisement to a destination d from a neighbour j. Sequence number, hop count and enhanced cumulative expected transmission count for a destination d at node i or node j are denoted by the variables $seqnum_i^d$, $hopcount_i^d$ and $enh\text{-}cetx_j^d$ respectively.

The LRODV protocol's route selection procedure is shown in Fig. 1. S and D stand for source and destination in this instance. Among the available paths S-B-E-I-D with enh-CETX=0.7, S-A-C-F-H-D with enh-CETX=0.9, and S-B-C-F-H-D with enh-CETX=0.9, the path S-A-F-H-D with enh-CETX=0.6 is chosen as the primary route for data transmission. The enhanced Expected Transmission Count (enh-ETX) of a link between the participating nodes along the path defined in terms of the amount of PROBE packets, and the least enhanced Cumulative Expected Transmission Count (enh-CETX) are the sole factors considered when selecting routes in LRODV.

4 Simulation environment and experimental results

The process of building a model for a real system and running experiments on it to compare various operating strategies or gain a better understanding of the system's behaviour is known as simulation [13]. Figure 2 illustrates the simulation model [14].

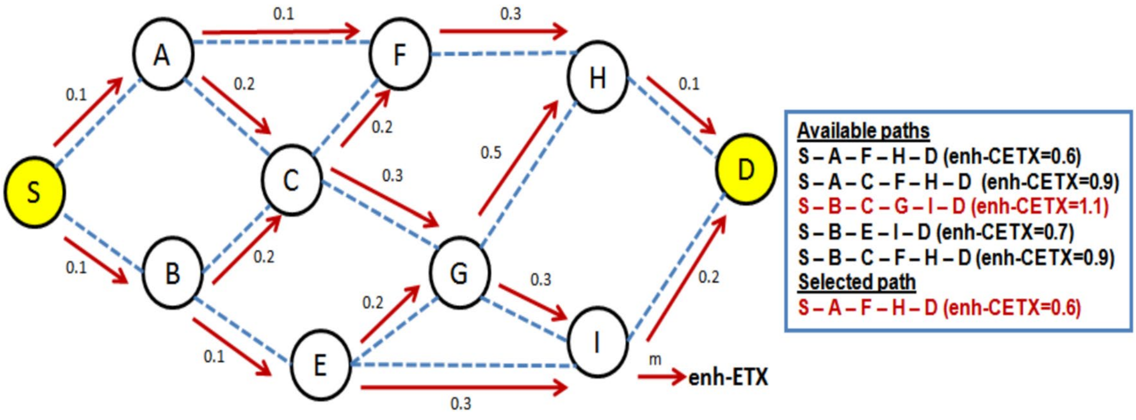


Fig. 1 Route selection process of LRODV protocol

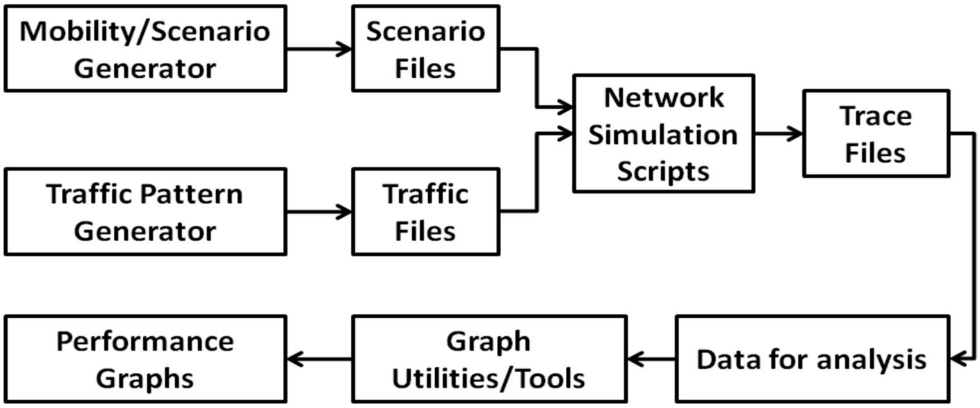


Fig. 2 Overview of the simulation model [14]

4.1 Environmental setup

With varying network flows on the widely used scenario pattern random way-point mobility (RWM) model [15] under CBR [16] traffic using NS2 [13, 17, 18], the performance of LRODV is compared with the commonly used unipath routing protocol AODV. The simulation parameters are shown in Table 6.

4.2 Performance metrics

Performance metrics are a group of qualitative measurements that are used to assess the quality of service (QoS) of any MANET routing protocol [19–24]. The seven distinct performance metrics that are listed below were assessed:

(i) The ratio of data packets created by the sources to those that are not delivered to the destination is known as the *packet loss ratio (%)*. The formula is as follows:

$$Packet\ Loss = (No.\ of\ Data\ pkts.\ Sent - No.\ of\ Data\ pkts.\ Received) \tag{5}$$

$$Packet\ Loss\ Ratio = \frac{Packet\ Loss}{No.\ of\ Data\ pkts.\ Sent} * 100 \tag{6}$$

(ii) The number of routing packets transported per data packet towards the destination during simulation is denoted by the phrase *normalised routing overhead (%)*. Here's how one obtains it:

$$Normalized\ Routing\ Overhead = \frac{No.\ of\ Routing\ pkts.\ Transmitted}{No.\ of\ Data\ pkts.\ Received} \tag{7}$$

(iii) The total energy consumed by all nodes in the simulation environment is given by the value *total energy consumed (in Joules)*. The following formula can be used to determine the total amount of energy used:

$$Total\ Energy\ Consumed = \sum_{i=1}^{n} (Initial\ Energy_i - Residual\ Energy_i) \tag{8}$$

(iv) The number of bytes received successfully is known as *Throughput (in Kbps)*. It is acquired through

$$Throughput = \frac{No.\ of\ Bytes\ Received * 8}{Simulation\ Time * 1000} kbps \tag{9}$$

(v) The ratio of data packets delivered to the destination to those generated by the sources is known as the *packet delivery ratio (%)*. The following formula is used to compute the Packet Delivery Ratio:

Table 6 Simulation parameters

Parameter(s)	Value(s)
Simulator	NS−2.35
MAC type	802.11 DCF
Simulation area	1520 m x 1520 m
Number of connections (network flows)	1, 5, 10, 20, 30, 40, 50 (Varying)
Routing protocols	LRODV & AODV
Traffic type	CBR (udp)
Data payload	512 bytes/packet
Network loads	4 packets/sec
Simulation time (in seconds)	300
Idle power	0.0001 W
Transmission power	1.0 W
Receiving power	1.0 W
Sleep power	0.0001 W
Transition power	0.002 W
Transition time	0.005 Sec
Initial energy	100 Joules
Interface queue length	50
Number of nodes	100
Pause time	10 sec
Speed	5 m/sec
Mobility models	Random waypoint mobility (RWM)

Table 7 Packet loss ratio (%) and Normalized routing overhead (%) of AODV & LRODV on RWM under CBR Traffic

Network flows	Packet loss ratio (%)		Normalized routing overhead (%)	
	AODV	LRODV	AODV	LRODV
1	0	0	0.083264	0.083264
5	0.621891	0.618684	0.720484	0.867192
10	17.187133	15.676044	2.877091	2.265537
20	45.271961	43.132184	7.071177	6.675088
30	63.419226	62.178623	10.863088	9.952544
40	65.686823	65.095737	11.104491	10.613224

Table 8 Total energy consumed (in Joules) and average end-to-end delay (in ms) of AODV & LRODV on RWM under CBR Traffic

Network flows	Total energy consumed (in Joules)		Average end-to-end delay (in ms)	
	AODV	LRODV	AODV	LRODV
1	9484.18	9384.06	12.411158	12.601932
5	6179.48	5985.23	12.475504	12.671003
10	2529.61	2749.34	12.680707	12.734009
20	1413.92	1355.91	12.841218	13.053741
30	970.11	944.12	13.154986	13.377584
40	947.23	975.52	13.180115	13.607537

$$Packet\ Delivery\ Ratio = \frac{No.\ of\ Data\ pkts.\ Received}{No\ of\ Data\ pkts.\ Sent} * 100 \tag{10}$$

(vi) The total amount of control or routing packets created by the routing protocol during simulation is known as *routing overhead (Pkts)* and is calculated as follows:

$$Routing\ Overhead = No.\ of\ RTR\ pkts. \tag{11}$$

(vii) The average time for a data packet to be successfully transferred over a MANET from source to destination is defined as the *average end-to-end delay (in ms)*. It covers all conceivable delays such as buffering during route discovery latency, queuing at the interface queue, retransmission delay at the MAC, propagation, and transfer time. It is determined as follows:

$$Average\ End-to-end\ Delay = \frac{\sum_{i=1}^{n}(R_i - S_i)}{n} \tag{12}$$

Where n is the number of data packets successfully transported across the MANET, 'i' represents the unique packet identifier, R_i represents the time when a packet with unique identifier 'i' is received, and S_i represents the time when a packet with unique identifier 'i' is sent. For high performance, the average end-to-end delay should be reduced.

Table 9 Packet delivery ratio (%) and throughput (in kbps) of AODV & LRODV on RWM under CBR Traffic

Network fows	Packet delivery ratio (%)		Throughput (in kbps)	
	AODV	LRODV	AODV	LRODV
1	100	100	16.411164	16.411164
5	99.378109	99.381316	65.480809	65.814839
10	82.812867	84.323956	96.316378	101.51164
20	54.728039	56.867816	104.603031	108.082317
30	36.580774	37.821377	92.84283	95.807128
40	34.313177	34.904263	92.143715	93.356765

Table 10 Routing overhead (in Pkts) of AODV & LRODV on RWM under CBR traffic

Network flows	Routing overhead (in Pkts)	
	AODV	LRODV
1	100	100
5	3454	4179
10	20,295	16,842
20	54,144	52,840
30	73,869	69,837
40	74,922	72,552

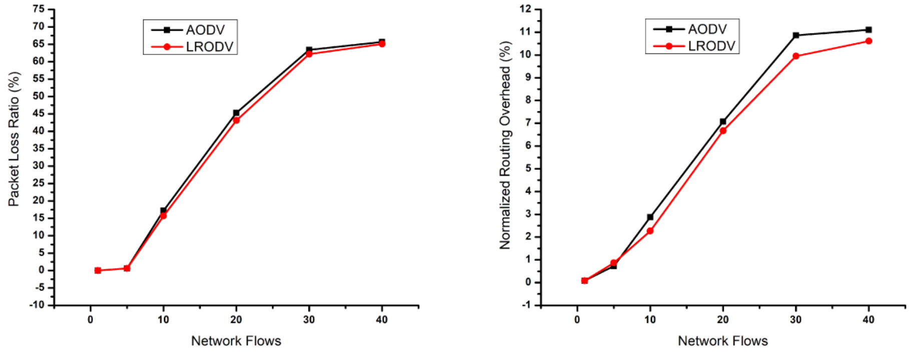
4.3 Experimental results and discussion

The performance of LRODV protocol is compared with AODV protocol with varying network flows on random way-point mobility (RWM) model under Constant Bit Rate (CBR) traffic pattern using NS 2.35 in terms of Quality of Service (QoS) metrics. When there is a hike in network flows, the LRODV reduces 4.822741 % of routing overhead as shown in Table 10 and Fig. 3f, 2.938256 % of packet loss ratio as shown in Table 7 and Fig. 3a, 7.429350 % of normalized routing overhead as shown in Table 7 and Fig. 3b and 0.609278 % of energy consumption as shown in Table 8 and Fig. 3c. Additionally, compared to the AODV routing protocol, it enhances throughput by 2.741449 % and packet delivery ratio by 2.938256 %, as indicated in Table 9 and Fig. 3e and d.

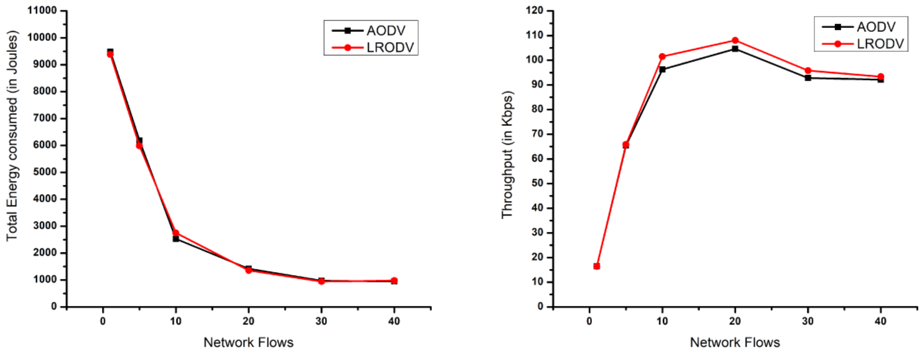
5 Conclusions and future work

Using NS 2.35, the performance of the LRODV and AODV protocols is compared in terms of quality of service (QoS) metrics with changing network flows on the random way-point mobility (RWM) model under the Constant Bit Rate (CBR) traffic pattern. The LRODV lowers 4.822741%

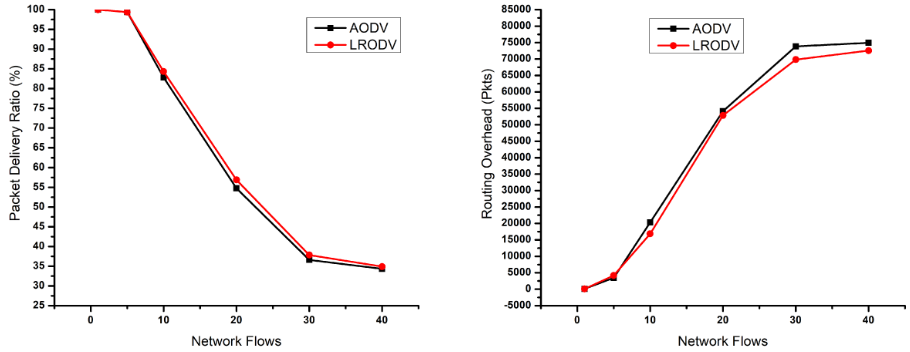
Fig. 3 Varying network flows in CBR traffic on RWM



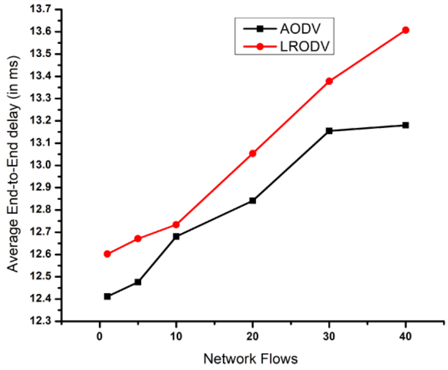
(a) Packet Loss Ratio (%) (b) Normalized Routing Overhead (%)



(c) Total Energy Consumed (Joules) (d) Throughput (Kbps)



(e) Packet Delivery Ratio (%) (f) Routing Overhead (Pkts)



(g) Average End-to-End delay (ms)

of routing overhead, 2.938256% of packet loss ratio, 7.429350% of normalised routing overhead, and 0.609278% of energy usage as network traffic increase. In comparison to the AODV routing protocol, it also boosts throughput by 2.741449% and packet delivery ratio by 2.938256%. The performance of the suggested protocol will also be evaluated in Cognitive Radio Ad hoc Networks due to its scope in link reliability, and in the future, the average end-to-end delay will be reduced by adding one or more unique routing metric.

Author Contributions The author formulated a new routing metric in this paper for ensuring route's link reliability for data transmission in mobile ad hoc networks.

Funding This research received no external funding.

Data availability Not Applicable.

Declarations

Conflict of interest Author declares no conflict or conflict of interest.

Ethical pproval The author declares that there is no conflict of interest regarding the publication of this paper

References

1. Abolhasan M, Wysocki T, Dutkiewicz E (2004) A review of routing protocols for mobile ad hoc networks. Ad Hoc Netw 2(1):1–22. https://doi.org/10.1016/S1570-8705(03)00043-X
2. Agrawal R, Faujdar N, Romero CAT, Sharma O, Abdulsahib GM, Khalaf OI, Mansoor RF, Ghoneim OA (2023) Classification and comparison of ad hoc networks: a review. Egypt Inform J 24(1):1–25. https://doi.org/10.1016/j.eij.2022.10.004
3. Roy AK, Khan AK (2020) Rtt based wormhole detection for wireless mesh networks. Int J Inform Technol 12(2):539–546. https://doi.org/10.1007/s41870-019-00417-4
4. Fragkoulis DG, Kouvakas ND, Koumboulis FN, Georgiou NI (2023) Modelling and modular supervisory control for the aodv routing protocol. AEU - Int J Electron Commun 169:154761. https://doi.org/10.1016/j.aeue.2023.154761
5. Sathyaraj P, Devi SR, Kannan K, Begum KJ, Sivalingam V, Jaiswal S (2023) Smart and secured data communication using modified aodv protocol over wireless communication network. AIP Conf Proc 2587:040002. https://doi.org/10.1063/5.0151546
6. Jiang Y, Sun H, Yang M (2023) Aodv-eocw: an energy-optimized combined weighting aodv protocol for mobile ad hoc networks. Sensors. https://doi.org/10.3390/s23156759
7. Mankotia V, Sunkaria RK, Gurung S (2023) Dt-aodv: a dynamic threshold protocol against black-hole attack in manet. Sādhanā. https://doi.org/10.1007/s12046-023-02227-8
8. Kukreja D, Sharma DK (2022) T-sea: trust based secure and energy aware routing protocol for mobile ad hoc networks. Int J Inform Technol 14(2):915–929. https://doi.org/10.1007/s41870-019-00392-w
9. Perkins CE, Royer EM (1999) Ad-hoc on-demand distance vector routing. In: Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications, pp. 90–100. https://doi.org/10.1109/MCSA.1999.749281
10. Johnson DB, Maltz DA (1996) In: Imielinski T, Korth HF (eds) Dynamic source routing in ad hoc wireless networks. Springer, Boston, pp. 153–181. https://doi.org/10.1007/978-0-585-29603-6_5
11. Almazok SA, Bilgehan B (2020) A novel dynamic source routing (dsr) protocol based on minimum execution time scheduling and moth flame optimization (met-mfo). EURASIP J Wirel Commun Netw. https://doi.org/10.1186/s13638-020-01802-5
12. Perkins CE, Bhagwat P (1994) Highly dynamic destination sequenced distance vector routing (dsdv) for mobile computers. In: ACM Computer Communication Review, Special Interest Group on Data Communication (ACM SIGCOMM'94) 24(4), 234–244 https://doi.org/10.1145/190314.190336
13. Issariyakul T, Hossain E (2008) Introduction to network simulator NS2
14. Periyasamy P, Karthikeyan E (2013) Performance comparison and evaluation of different multipath routing protocols based on various scenario and traffic patterns for mobile ad hoc networks. Int J Comput Netw Inform Secur (IJCNIS) 5(1):24–32. https://doi.org/10.5815/ijcnis.2013.01.03
15. Roy RR (2016) Handbook of mobile ad hoc networks for mobility models
16. Kakkar P, Singla V (2010) Traffic pattern based performance comparison of reactive and proactive protocols of mobile ad-hoc networks. Int J Comput Appl 5(10):16–20. https://doi.org/10.5120/949-1090
17. The Network Simulator - Ns-2. https://www.isi.edu/nsnam/ns/
18. Fall K, Varadhan K. The Network Simulator Ns-2: Documentation. https://www.isi.edu/nsnam/ns/ns-documentation.html
19. Camp T, Boleng J, Davies V (2002) A survey of mobility models for ad hoc network research. Wirel Commun Mob Comput 2(5):483–502. https://doi.org/10.1002/wcm.72
20. Periyasamy P, Karthikeyan E (2017) End-to-end link reliable energy efficient multipath routing for mobile ad hoc networks. Wirel Pers Commun 92(3):825–841. https://doi.org/10.1007/s11277-016-3579-z
21. Saini H, Garg AK (2022) To investigate an efficient resilience oriented routing mechanism for high speed networks. Int J Inform Technol 14(1):569–578. https://doi.org/10.1007/s41870-018-0089-0
22. Chiwariro R, Thangadurai N (2022) Quality of service aware routing protocols in wireless multimedia sensor networks: survey. Int J Inform Technol 14(2):789–800. https://doi.org/10.1007/s41870-020-00478-w
23. Mahapatra B, Patnaik S (2019) An analysis on data reduction methods for manets to reduce incoming data as a preprocessing technique. Int J Inform Technol 11(1):75–88. https://doi.org/10.1007/s41870-018-0170-8
24. Chander D, Kumar R (2022) Multicast error correction method to support scalability in mobile ad hoc networks. Int J Inform Technol 14(1):491–506. https://doi.org/10.1007/s41870-018-0164-6