(12) PATENT APPLICATION PUBLICATION
(19) INDIA
(22) Date of filing of Application :13/03/2025
(21) Application No.202531022900 A
(43) Publication Date : 04/04/2025

(54) Title of the invention : Adaptive Multi-Verse Optimization-Based Secure Routing Algorithm for Vehicular Ad Hoc Networks

(51) International classification :H04L0009400000, H04L0009320000, H04L0043160000, H04L0045280000, H04W0040120000
(86) International Application No :NA
Filing Date :NA
(87) International Publication No : NA
(61) Patent of Addition to Application Number :NA
Filing Date :NA
(62) Divisional to Application Number :NA
Filing Date :NA

(71)**Name of Applicant :**
**1)Rahul Kumar Singh**
Address of Applicant :Patna. Bihar ---------- ----------
**2)Sumit**
**3)Rajender Singh Chhillar**
**4)Sandeep Dalal**
**Name of Applicant : NA**
**Address of Applicant : NA**
(72)**Name of Inventor :**
**1)Sumit**
Address of Applicant :Maharshi Dayanand University, Rohtak, Haryana, India-124001 ---------- ----------
**2)Rajender Singh Chhillar**
Address of Applicant :Maharshi Dayanand University, Rohtak, Haryana, India-124001 ---------- ----------
**3)Sandeep Dalal**
Address of Applicant :Maharshi Dayanand University, Rohtak, Haryana, India-124001 ---------- ----------
**4)Rahul Kumar Singh**
Address of Applicant :K. R. Mangalam University, Gurugram, Haryana, India-122103 Sohna ---------- ----------

(57) Abstract :
This invention introduces a secure, adaptive, and optimized routing method for VANETs using multi-verse optimization (MHDORA) to enhance performance and mitigate Man-in-the-Middle (MITM) attacks. The proposed method dynamically selects the most secure and efficient path by analyzing real-time network conditions, traffic loads, and security risks. A real-time anomaly detection mechanism identifies potential attacks and triggers adaptive rerouting, ensuring uninterrupted communication. Additionally, a hybrid cryptographic security framework integrates SSL/TLS encryption, digital signatures, and two-factor authentication (2FA) to safeguard data integrity and prevent unauthorized access. The system further employs blockchain-based trust management to authenticate routing interactions, preventing route manipulation and malicious node interference. Experimental results demonstrate superior performance in latency reduction, packet delivery rate, and attack resilience compared to existing methods like HDORA, DORA, an

No. of Pages : 15 No. of Claims : 4