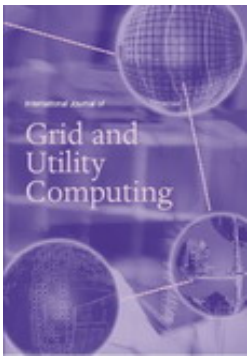
INDERSCIENCE PUBLISHERS
Linking academia, business and industry through research



International Journal of Grid and Utility Computing

ISSN online: 1741-8488 - ISSN print: 1741-847X
https://www.inderscience.com/ijguc

Hybrid optimisation-based reliable routing with traffic management and congestion control

Kaveri Kori, Sridevi Hosmani

DOI: 10.1504/IJGUC.2024.10067188

Article History:

Received:	10 November 2023
Last revised:	13 February 2024
Accepted:	01 March 2024
Published online:	12 January 2025

Hybrid optimisation-based reliable routing with traffic management and congestion control

Kaveri Kori

Department of Computer Science and Engineering,
Sharnbasva University,
Kalaburagi, Karnataka, India
Email: kaverikori1412@gmail.com

Sridevi Hosmani*

Department of Artificial Intelligence and Machine Learning,
Sharnbasva University,
Kalaburagi, Karnataka, India
Email: hosmani.sridevi@gmail.com
*Corresponding author

Abstract: Reliable routing with traffic management in VANET is the most critical aspect to be solved on an emergency basis. There is a need for a trust computing system adapted to the peculiarities of VANETs to deal with the significant factors of road safety. The purpose of this work is to suggest a new improved trust-based methodology for dependable transmission. To transmit the data packet efficiently, the cluster head selection and optimal routing process takes place. The Fuzzy C-Means Clustering (FCM) technique is employed to select the cluster head, in which the node with high energy is selected as the cluster head. Followed by, a novel hybrid optimisation named the Beluga Whale-Assisted Coati Optimisation (BWACO) algorithm is proposed, which is the combination of the Beluga Whale Optimisation (BWO) and Coati Optimisation Algorithm (COA). The greatest mobility offered using the BWACO approach is –146.386 at the median statistical metric.

Keywords: trust-based protocol; traffic; energy; distance; mobility.

Reference to this paper should be made as follows: Kori, K. and Hosmani, S. (2025) 'Hybrid optimisation-based reliable routing with traffic management and congestion control', *Int. J. Grid and Utility Computing*, Vol. 16, No. 1, pp.41–59.

Biographical notes: Kaveri Kori has completed her Bachelor of Engineering degree from Appa Institute of Engineering and Technology in 2016 and Completed her MTech in 2018 and currently working as an Assistant Professor in the Department of MCA, Sharnbasva University. She has attended five days FDP workshop on Artificial Intelligence and Machine Learning. Her research interest is in the area of vehicular ad-hoc networks.

Sridevi Hosmani is working as an Associate Professor in the Department of Artificial Intelligence and Machine Learning and completed her PhD degree in the year 2021 from Vishweshwarayya University. She has published 15 papers in international journals, attended 3 international conferences, has 2 patents, selected 2 sponsorship projects and attended more than 50 workshops.

1 Introduction

The global total quantity of automobiles on the road is increasing at an alarming rate. This results in altering the circumstances of driving, and also causes potentially dangerous circumstances for driving. Accidents, in particular, are becoming more common, which leads to bodily injuries and deaths. Moreover, drivers are additionally discovering it more challenging to make it to their intended destinations due to heavy traffic. Therefore, there is tremendous demand for drivers to be aided through assistance programs and control systems to improve their road safety, especially, when significant occurrences including accidents, terrible weather conditions, traffic jams and so on occur. Also, academic researchers and automotive manufacturers are making progress regarding inter-vehicle communications-based applications delivered via VANETs (Ahmed et al., 2018; Gazdar et al., 2018; Ghajar et al., 2021). VANET constitutes an autonomously organised network that is a critical component of Intelligent Transport System (ITS). Further,

VANET uses two modes of communication, Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I), to allow vehicles to connect immediately to nearby vehicles and RSUs (Khan et al., 2019; Liu et al., 2020; Li et al., 2021). Also, it improves traffic efficiency, transportation security as well as neighbourhood services.

Vehicles are going to work together in VANETs to gain advantages from an extensive variety of applications. Nonetheless, the transparent structure of the vehicle context renders it unavoidable and subject to a variety of security vulnerabilities. Also, this encourages vehicles to exercise caution while collaborating with others in the field. Moreover, vehicles send out notifications or brief messages when there is an emergency on the road. Authorities must then verify not just the device that is sending these communications, but additionally the information that was received, because a valid node may broadcast fake data. For example, a hostile vehicle may alter data about an actual incident, including the time of occurrence, the location, and so on, or it may manufacture false incidents that are not real with the objective to disrupt the behaviour of other drivers. Nevertheless, because of the distinctive attributes of VANET (Abassi et al., 2020; Gazdar et al., 2022; Inedjaren et al., 2021), including dynamic connections and high mobility, it is susceptible to a wide range of internal and external attacks. As a result, trust-based VANET routing topologies are developed (Hasrouny et al., 2019; Yan et al., 2021; Chukwuocha et al., 2021). Particularly, Artificial Intelligence models are applicable as the routing protocols to deal with the conditions to be considered in this sector. When there are many vehicles communicating at once, there is channel saturation and data congestion, which raises data loss, packet latency and service quality quickly. Various traditional implementations have been put up to support urban VANETs in enhancing the junction-aided routing choice (Hemmati et al., 2024; Azzoug and Boukra, 2024). One of the primary reasons that adversely affect the Inter-Vehicle Communication (IVC) efficiency of such emerging networks in Vehicular Ad Hoc Networks (VANETs) is congestion. Because VANETs are dynamic networks with highly mobile vehicles and frequent link disconnections, secure routing methods are necessary to create dependable and effective communication channels (Abdollah and Zarei, 2021; Azizi and Shokrollahi, 2024).

On the other hand, traffic management frameworks have been presented as a new approach to determining the minimum degree of safety amongst collaborating nodes. Also, trust systems focus on computing knowledge itself, enabling data dependability to be validated. Other network security functions provided by trust systems include authentication, access control, secure exchange of resources and malicious vehicle detection. As a result, it is critical to verify the dependability of vehicles regularly utilising computational approaches and metrics. Many trust processing approaches for VANET were built, however they did not produce enhanced outcomes. As a result, a novel enhanced trust-based protocol for VANETs is being suggested.

The main contributions are:

- Contributes a Fuzzy C-Means clustering (FCM) technique for cluster head selection to assure reliable routing, in which the vehicle with high energy is considered as the cluster head.
- Proposes a hybrid optimisation approach named BwACO algorithm, in which the Coati Optimisation Algorithm (COA) collaborates with Beluga Whale Optimisation (BWO) to select the route optimally under the consideration of constraints like energy, distance, mobility, delay, trust and link quality.
- Determines a traffic management and congestion control approach with regard to vehicles which are leaving the cluster and vehicles which are joining the cluster.
- Contributes a reliable retransmission approach, and enables the sender to retransmit only the missing packets by lowering the unnecessary retransmission.

The structure is as follows:

A review of traditional techniques with regard to trust-based protocol for VANET is given in Section 2. The proposed model of enhanced trust-based protocol is discussed in Section 3. The analysis of different approaches is given in Section 4. Finally, the conclusion is given in Section 5.

2 Literature review

Gazdar et al. (2018) proposed a novel distributed trust computing system adapted to the peculiarities of VANETs and aimed at addressing the aforementioned difficulties. They also presented a tier-based message distribution approach to detect eavesdropped communications and false events more efficiently. Each vehicle verified the veracity of the incoming data packets and maintained a trust value for each of its neighbours. They simulated the growth of harmful vehicles' trust metrics analytically.

Zhang et al. (2020) suggested an Anti-Attack Trust Management Scheme (AATMS) in VANET to assess vehicle dependability in VANET might avoid harmful vehicles and collaborate with trusted vehicles with the use of AATMS. In the beginning, Bayesian inference was used to compute vehicle local trust based on past encounters. Then, they chose a limited group of seed vehicles based on local trust and other social considerations.

Tangade et al. (2020) suggested a Trust Management scheme based on Hybrid Cryptography (TMHC) to strengthen VANET security. Since trust-building and secure communication between cars depend on authentication, the suggested TMHC uses hybrid cryptography-based authentication for a reliable and effective trust management system. Hybrid cryptography included both symmetric Hash Message Authentication Code (HMAC) and asymmetric ID-based digital signature. To verify the suggested approach, the results were obtained by extensive simulations.

Rehman et al. (2022) developed a novel trust architecture that addressed most of the characteristics of trust in IoV to effectively detect events and malicious nodes. The framework learnt the surroundings intellectually from the received information and constructed a context around an occurrence. Aside from Trust Management (TM), the proposed system included a unique method for detecting malicious nodes based on anomalous outliers. An experimental simulation was used to evaluate the framework's performance. The findings reveal that performance metrics were improving.

Ahmad et al. (2018) offered an innovative TEAM framework that functioned as a novel paradigm for the design, administration and assessment of TMs in varied circumstances and in the presence of malevolent vehicles. The developed framework was tested with the installation of three distinct types of TMs in four different VANET scenarios based on the mobility of both malicious and honest vehicles. The results showed that the Trust Evaluation and Management (TEAM)was capable of simulating a wide range of TMs, with the efficiency measured against several QoS and security-related parameters.

In Malik et al. (2020), a novel trust management system with two primary phases: protected message transmission and node trustability prediction, was introduced. The data sanitisation procedure was used to ensure message security by applying the privacy preservation approach. A novel hybrid algorithm called Sea Lion Explored-Whale Optimisation Algorithm (SLEWOA), which was a mix of Whale Optimisation Algorithm (WOA) and Sea Lion Optimisation Algorithm (SLOA), was utilised to optimise the key used in the sanitisation process. Finally, for particular measurements, the suggested model's performance was tested and proven to be superior to other traditional techniques.

Poongodi et al. (2019) built a framework based on trust with a fresh technique to detect DDoS assaults in VANET. The trust evaluation matrix was generated based on the trust factors. They created the trust mechanism in a unique way to provide improved security by preventing trespassers in the network. The proposed solution maximised bandwidth consumption without jeopardising network node security.

Kudva et al. (2021) demonstrated the block chain-based decentralised trust score system for participating nodes to detect and blacklist insider attackers in VANET proactively. They suggested a two-stage detection method, with surrounding nodes calculating trust individually at the first level. A consortium block-chain-based system with approved RSUs as validators aggregate trust scores for vehicle nodes at the second level. Finally, they demonstrated that the suggested solution enhanced VANET performance by reducing and blacklisting insider attack-initiating nodes.

Sataraddi and Kakkasageri (2020) framed trust and delay-based routing protocol to preserve the network from malicious attacks. Between the Message Reachable Time (MRT) and vehicles, the suggested work is implemented by considering the trust evaluation. The vehicles with less MRT and greater trust factor were considered in the route selection. In contrast with the Delay-aware and Backbone-based Geographic Routing (DBGR), the overall performance of the presented model was implemented.

Habelalmateen et al. (2022) framed the TACRP model to enrich traffic management by utilising low-energy consumption in the network. By aiding Road Side Units (RSUs), the traffic management unit was established to manage the whole network. To enhance the stability of the network, the vehicles with equivalent direction and speed were collected into a cluster and thus minimising the networks' energy consumption. Thereby, this network provided a significant grouping of vehicles on the road.

Kaur and Kakkar (2022) developed a Deep Maxout Network (DMN) for attack categorisation in VANET using hybrid optimisation. Designed hybrid optimisation approach is used for Cluster Head (CH) selection and routing. To carry out the classification process effectively, the feature selection procedure is very important. Furthermore, DMN is used to classify attacks, and an optimisation approach is introduced to teach it. Better classification performance, with precision and recall of 0.9395 and 0.9462, as well as routing performance, with energy and trust of 0.2454J and 0.4402, were obtained by the created optimisation-based DMN model.

Souri (2022) developed the technical examination of Artificial Intelligence (AI) techniques for connectivity management systems in Internet of Things (IoT) environments is presented in this research. This paper offers a thorough analysis of vehicular communication systems, Vehicular Ad Hoc Networks (VANETs) and Internet of Vehicles (IoV) techniques that have been assessed utilising intelligent algorithms, fuzzy logic and machine learning. Additionally, successful learning models, applicable assessment metrics to anticipate and identify effective connectivity strategies, and the improvement of IoT-based connectivity management systems are explored and examined for current AI methodologies. Lastly, new avenues for study and arising issues are discussed in order to enhance the functionality of sophisticated IoT-based connectivity management systems.

Kadam et al. (2023) introduced the innovative Trust Aware Clustering-based Routing Protocol (TACR) to minimise computational costs and latency while addressing security and reliability issues in VANET connections. As the name implies, effective trust-management strategies are critical to the optimal selection of relay (data forwarder) and Cluster Head (CH) for TACR operation. During the grouping stage, we compute the direct and indirect trust scores for each automobile in each cluster. We use the hybrid trust value of each vehicle as a consequence of the Ant Colony Optimisation (ACO) method's fitness function.

2.1 Problem statement

Table 1 reveals the benefits and limitations of extant approaches relevant to routing with traffic management and congestion control in VANETs. The Enhanced Distributed Trust Computing Protocol (EDTCP) (Gazdar et al., 2018) approach virtually recognises all malicious vehicles and measures of trust were often updated based on the

authenticity of the received messages; however, enhancing the performance of VANET, it didn't adopt ML approaches for effective estimation of trust metrics is complicated. The Anti-Attack Trust Management Scheme (AATMS) (Zhang et al., 2020) achieved robustness by adopting Bayesian inference and TrustRank to estimate local and global trust values of vehicles, respectively; however, it is necessary to improve the link assessment strategy to compute the global trust of vehicles. The Trust Management scheme based on Hybrid Cryptography (TMHC) (Tangade et al., 2020) scheme ensures the privacy perseverance of vehicles through pseudo-identity; however, deploying RSU or other distinct approach with ATA access coupled with V2V is difficult. The CTMF (Rehman et al., 2022) employs outlier techniques to detect malicious vehicles in a network; however, adopting ML with big data to employ as supportive equipment for long-term trust control. The TEAM (Ahmad et al., 2018) approach ensured the dissemination of trusted messages in terms of both data-oriented and hybrid TMs; however, work on numerous TMs along with TEAM to preserve from attack is difficult. The SLE-WOA (Malik et al., 2020) scheme performed security-assured messages by incorporating a privacy preservation system; however, improving the key sensitivity is difficult. The trust-based scheme (Poongodi et al., 2019) attained high trust evaluation; yet, it is difficult to employ any integrated message confirmation approaches techniques for efficiently organising the confidentiality of the system. The Blockchain-based trust score management system (Kudva et al., 2021) efficiently disseminates the message by avoiding the blackhole nodes; however, implementing ML or DL schemes for the better performance of trust score organisation is difficult.

Table 1 Features and challenges of extant approaches relevant to routing with traffic management and congestion control in VANETs

Author [Citation]	*Methodologies*	*Features*	*Challenges*
Gazdar et al. (2018)	EDTCP	The measures of trust were often updated based on the authenticity of the received messages.	To enhance the performance of VANET, it didn't adopt ML approaches for effective estimation of trust metrics.
Zhang et al. (2020)	AATMS	It achieved robustness by adopting Bayesian inference and TrustRank to estimate local and global trust values of vehicles, respectively.	Though, it needed improvement in link assessment strategy to compute the global trust of vehicles.
Tangade et al. (2020)	TMHC	It ensures the privacy perseverance of vehicles through pseudo-identity.	Need to deploy RSU due to limited urban areas; otherwise, employ a distinct approach with ATA access coupled with V2V.
Rehman et al. (2022)	CTMF	By employing an outlier technique, this presented model detected malicious vehicles in a network.	It didn't adopt ML with big data to employ as supportive equipment for long-term trust control.
Ahmad et al. (2018)	TEAM	It ensured the dissemination of trusted messages in terms of both data-oriented and hybrid TMs.	Need to work on numerous TMs along with TEAM to preserve from attack.
Malik et al. (2020)	SLE-WOA	It performed security-assured messages by incorporating a privacy preservation system.	It is necessary to improve the key sensitivity since it generates 17% of raw data with the key variation of 10%.
Poongodi et al. (2019)	Trust-based mechanism	It attained a high trust evaluation.	It didn't employ any integrated message confirmation approaches or techniques for efficiently organising the confidentiality of the system.
Kudva et al. (2021)	Blockchain-based trust score management system	It efficiently disseminates the message by avoiding the blackhole nodes.	It didn't implement with ML or DL schemes for the better performance of trust score organisation.
Sataraddi and Kakkasageri (2020)	Trust and delay-based routing	It attained better throughput and PDR.	Need to consider QoS parameters like link longevity of nodes and signal strength to recognise malicious node.
Habelalmateen et al. (2022)	TACRP	It enhances the stability of the network with low energy consumption.	It didn't adapt the system to numerous multifaceted circumstances.

3 An overview of enhanced trust-based protocol for VANET with traffic management and congestion control-based reliable routing

3.1 System model

The framework of VANET comprised of three major elements namely, Road Side Unit (RSU); vehicles furnished with On Board Unit (OBU) and Trusted Authority (TA). Assume that the vehicles be $\wp_i$, which are represented as collection of mobile nodes furnished with OBU. The OBU in vehicles aids in communicating with RSU and other vehicles. The trust rates are estimated for each vehicle and send newly produced rate of local trust to RSUs. Through wireless communication, the RSU gathers the rate of local trust from $\wp_i$, which is the main responsibility of the RSU and it offers the rate of local trust to the TA via the network. To gather sufficient trust data, the RSU is generally employed at significant transportation hubs including exit high-speed and street intersections. Moreover, each vehicle is verified with its authenticity via TA and also it takes charge of estimating the rate of vehicles' global trust. With the local trust rate obtained from RSU, the standard rate of global trust and social parameters, the rate of vehicles' global trust is estimated. Also, the TA has enough memory storage as well as estimating resources. The OBU has no authenticity to control the vehicles when compared to the other two elements like RSU and TA. Hence, there is a possibility for the vehicle with untrustworthy. To address this issue, an enhanced trust-based protocol is designed with the following three steps: (i) the routing process is performed via cluster head selection and optimal routing. The FCM approach is employed to select the cluster head and proposed an innovative optimisation strategy called the Beluga whale Assisted in Coati Optimisation (BwACO) Algorithm for choosing the optimal route taking into account limitations such as energy, distance, mobility, latency, link quality and trust; (ii) The traffic management and congestion control process is performed under the consideration of vehicle which is leaving the cluster and vehicle which are joining the cluster. (iii) Finally, a reliable transmission process is performed by considering the following stages like packet transmission, acknowledgement, retransmission and maximum retransmission attempts.

3.2 FCM-based clustering (Cluster head Selection) & BwACO algorithm for optimal route selection

The procedure of establishing the path for data transmission between source and destination via the network is termed as routing. The primary goal of this routing is to maximise certain limitations while allowing the data packets to reach their destination. To ensure network reliability, performance and security, implementing efficient routing is important. Hence, this work ensured efficient routing protocol by deploying the FCM approach and hybrid optimisation strategy. The FCM approach is employed for cluster head selection and the hybrid optimisation strategy BwACO algorithm is employed for optimally choosing routing. Figure 1 shows the ideal routing process using BwACO.

3.2.1 Cluster head selection: FCM

FCM (Zhou and Yang, 2019) is a clustering algorithm that is employed in this work, to select the cluster head in the VANET environment. In VANET, there are vehicles that are considered as mobile nodes such that $\wp_i : i \to \{1, 2, ..., V\}$ with V number of vehicles. Initially, the clusters are determined along with electing original cluster centre's arbitrarily. Followed by the estimated membership degree of all nodes $\wp_i$ to cluster c_j and it is updated frequently. The updated form of membership degree φ_{ij} of all nodes $\wp_i$ to cluster c_j is estimated according to equations (1) and (2).

$$\varphi_{ij} = \frac{1}{\sum_{q=1}^{p}\left[d\left(\wp_i, c_j\right)/d\left(\wp_i, c_r\right)\right]^{2/m-1}} \tag{1}$$

$$c_j = \frac{\sum_{i=1}^{V} \varphi_{ij}{}^{m} \wp_i}{\sum_{i=1}^{V} \varphi_{ij}{}^{m}} \tag{2}$$

where m represents fuzzifier vector, and $d\left(\wp_i, c_j\right)$ represents Euclidean distance of nodes $\wp_i$ to cluster c_j. The objective function is computed for each iteration according to equation (3).

$$Obj^{FCM} = \sum_{i=1}^{V}\sum_{j=1}^{V} \varphi_{ij}{}^{m} \left\|\wp_i - c_j\right\|^2 \tag{3}$$

The FCM is used for each node in order to choose the cluster head. Selecting the cluster head is based on the energy value. The cluster head is the node that has the highest energy value. Additionally, Table 2 illustrates the limits related to energy, distance, mobility, delay, trust and link quality.

Table 2 Constraints for selecting optimal routing

Constraints	*Description*	*Formulae*
Energy	The amount of energy present in individual node for reliable transmission.	$Enr = Mean\left(Enr_{CH}\right)$ where Enr_{CH} represents remaining energy of cluster head node.
Distance	The distance from each cluster head to RSU by employing Euclidean distance.	$D_{CH-RSU} = \sqrt{\left(x_1 - x_2\right)^2 + \left(z_1 - z_2\right)^2}$ $Dis = Mean\left(D_{CH-RSU}\right)$ where $\left(z_1, z_2\right)$ represents coordinates of RSU and $\left(x_1, x_2\right)$ represents coordinates of cluster head nodes.
Delay	Delay refers to time taken for data transmission between source and destination. Also, it measures the spending time of data packet within a node.	$Dly = Dis/Speed$
Mobility	It measures the movement of node (vehicles) within the network for reliable transmission. Also, it is dependent on RSSI.	$RSSI = -36 * \log\left(Dis\right) - 55\right)$
Link quality	The quality of data packets received at the destination side. The link quality is verified by employing PLR. The data packets with low PLR determine good link quality.	$PLR = 1 - PDR$ $PDR = Rp/Sp$ where Sp represents the number of packets transmitted by the sender and Rp represents the number of successfully received packets.
Trust	It measures the reliability and level of confidence of a node. It is divided into two types: Direct trust and Advised trust.	Direct trust: $T_{Dir} = Round\left(\frac{\sum_{j=1}^{V}\left(G_j\right)\left(K_j^{(+)}\right)}{K_t}\right)$ *Advised trust*: $T_{Adv} = 1/n \sum_{j=1}^{V}\left(T_{Dir_j}\right)\left(TV_j\right)$ *Mixed trust*: $T_{Mix} = T_{Dir} + \left(1 + T_{Dir}\right)T_{Adv}$ where j is the knowledge, K_t is the total number of knowledge, $K_j^{(+)}$ is the positive knowledge TV_j is the trust value and G_j is the weight of knowledge.

3.2.2 Objective function

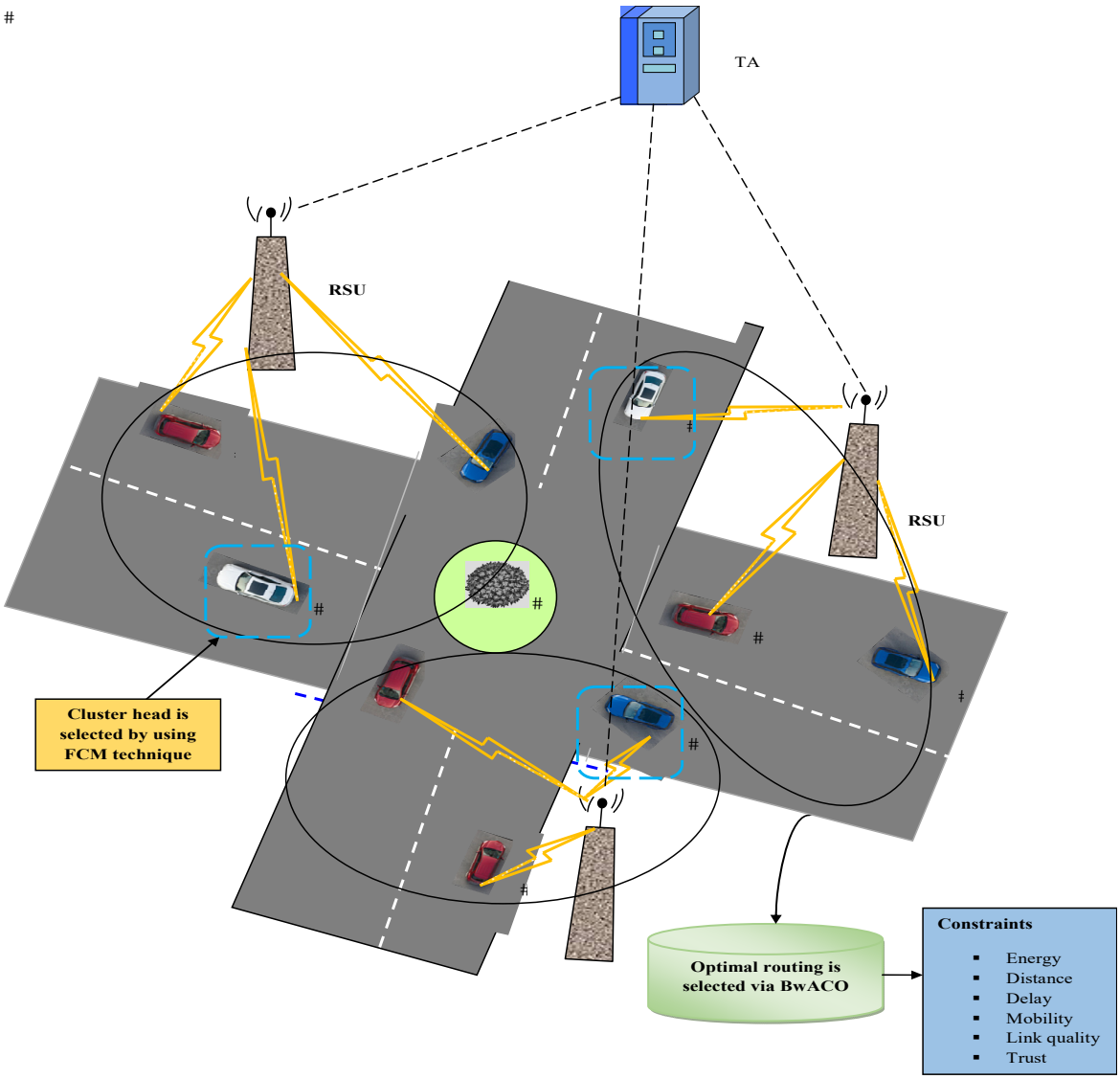
Equation (4) defines the objective function that is used by the suggested hybrid optimisation BwACO algorithm.

$$Fit = \left(w_1 * Dis\right) + \left(w_2 * \left(1 - Enr\right)\right) + \left(w_3 * \left(1 - T_{Mix}\right)\right) + \left(w_4 * \left(1 - PLR\right)\right) + \left(w_5 * \left(1 - Mobility\right)\right) + \left(w_6 * Dly\right) \quad (4)$$

where w_i are the weights such that $w_i : i \to \{1, 2, 3, 4, 5, 6\}$, here, w_1 is the weighting factor of distance, w_2 is the weighting factor of energy, w_3 is the weight factor of trust, w_4 is the weight factor of link quality, w_5 is the weight factor of mobility and w_6 is the weight factor of delay. The weight factor is estimated according to equation (5). Figure 1 depicts the optimal routing procedure via BwACO algorithm.

$$w_i = \frac{Constraints\left(i\right)}{Sum\left(Constraints\right)}; \quad \sum w_i = 1 \quad (5)$$

Figure 1 Optimal routing procedure via BwACO algorithm (see online version for colours)



3.2.3 Proposed hybrid optimisation BwACO algorithm for optimal routing

To select the optimal routing, the hybrid optimisation strategy is deployed. The hunting and escaping behaviour of coati are inspired for optimal selection of routing. The green iguanas (large lizards) are the favourite food of coati. The coati attack iguanas and escape from other creatures are the smart procedures. However, the convergence speed is a challenging issue. To address this issue, another meta-heuristic algorithm named BWO (Zhong et al., 2022) is employed in this work. Then the combined form of both coati and beluga behaviours are deployed in the innovative hybrid optimisation strategy BwACO algorithm. The proposed hybrid optimisation BwACO flow diagram is illustrated in Figure 2.

3.2.4 Solution encoding

The solution encodes into the hybrid optimisation strategy BwACO is the vehicle $\wp_i : i \to \{1, 2, ..., V\}$ to optimally select the reliable routing.

3.2.5 Mathematical modelling

The coati are considered to be vehicles as population members. The rate of decision variables is determined in search space through the position of all coatis. Also, the position of the coati is considered to be a candidate solution towards the issue. Firstly, the coatis are positioned arbitrarily according to equation (6). Here, C_i refers to the position of i-th coati in problem space, M refers to set of decision variables, N refers to total set of coatis, U_{b_j} refers to upper limit, L_{b_j} refers to the lower limit and r refers to arbitrary number between the interval 0 and 1.

$$C_i : c_{i,j} = L_{b_j} + r.\left(U_{b_j} - L_{b_j}\right) \quad i = 1, 2, ..., N; \quad j = 1, 2, ..., M \tag{6}$$

The population matrix includes the population of coatis that is represented according to equation (7).

$$C = \begin{bmatrix} C_1 \\ \vdots \\ C_i \\ \vdots \\ C_N \end{bmatrix}_{N\times M} = \begin{bmatrix} c_{1,1} & \cdots & c_{1,j} & \cdots & c_{1,M} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ c_{(i.1)} & \cdots & c_{(i.j)} & \cdots & c_{(i.M)} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ c_{(N.1)} & \cdots & c_{(N.j)} & \cdots & c_{N\times M} \end{bmatrix} \quad (7)$$

In decision variables, the position of the candidate solution evolves to estimate the distinct rates for the objective function according to equation (8).

$$Fit = \begin{bmatrix} F_1 \\ \vdots \\ F_i \\ \vdots \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F(C_1) \\ \vdots \\ F(C_i) \\ \vdots \\ F(C_N) \end{bmatrix}_{N\times 1} \quad (8)$$

where F is the objective function vector as per equation (9) and $F(C_1)$ refers to the value of the objective function. The updating position and procedure of coati is designed with two behaviours namely, attacking iguana strategy and escaping strategy form predators.

Improved attacking strategy on Iguana: A coati community climbs a tree to catch an iguana. Some of the coati community lurk underneath a tree till the iguana drops to the floor. Once the iguana drops to the floor level, the coatis approach it and kill it. Such a method makes coatis relocate towards diverse places in the exploration space illustrating the COA's (Dehghani et al., 2023) exploratory capabilities in global search in solving issues area. The position of coati in the tree to attack the iguana is modelled as in equation (10).

$$C_i^{P1} : c_{i,j}^{P1} = c_{i,j} + r\left(Ig_j - Int.c_{i,j}\right) \quad (9)$$

$$\text{For } i = 1,2,...,\lfloor N/2 \rfloor \text{ and } j = 1,2,...,M \quad (10)$$

The above equation (10) is improved to obtain the optimal position of coati (vehicle) optimally. Hence, the best position of the beluga is considered according to equation (11).

$$C = r_3 c_{best} - r_4.c_{ij} + J.Lf\left(c_r - c_{ij}\right) \quad (11)$$

Then, the new updation in BwACO is as follows in equations (12) to (16). Where $J = 2r_4\left(1 - t/t^{\text{Max}}\right)$ refers to jump strength, r_3 and r_4 are refers to arbitrary rate between 0 and 1 such that $r \in (0,1)$ and $Int \in (0.1,2)$; t^{Max} refers to maximum epoch and t refers to the current epoch.

$$C_{new} = \frac{c_{i,j}^{P1} + C}{2} \quad (12)$$

$$C_{new} = \frac{1}{2}\left[c_{ij} + r.\left(Ig - Int.c_{i,j}\right) + r_3 c_{best} - r_4.c_{ij} + J.Lf\left(c_r - c_{ij}\right)\right] \quad (13)$$

$$C_{new} = \frac{1}{2}\left[c_{ij} + r.Ig - r.Int.c_{i,j} + r_3 c_{best} - r_4.c_{ij} + c_r.J.Lf - c_{ij}.J.Lf\right] \quad (14)$$

$$C_{new} = \frac{1}{2}\left[c_{ij} - r.Int.c_{i,j} - r_4.c_{ij} - c_{ij}.J.Lf + r.Ig + r_3 c_{best} + c_r.J.Lf\right] \quad (15)$$

$$C_{new} = \frac{1}{2}\left[c_{ij}\left(1 - r.Int - r_4 - J.Lf\right) + r.Ig + r_3 c_{best} + c_r.J.Lf\right] \quad (16)$$

The iguana is placed in an arbitrary position when the iguana drops to the ground. In accordance with the arbitrary position, the coatis positioned in the ground shift towards the problem space is referred in equations (17) and (18). Here, Ig_G refers to the iguana available in the ground.

$$Ig_G : Ig_G = L_{b_j} + r.\left(U_{b_j} - L_{b_j}\right) \quad (17)$$

$$C_i^{P1} : c_{i,j}^{P1} = \begin{cases} c_{i,j} + r\left(Ig_{Gj} - Int.c_{i,j}\right) & ; \quad F_{Ig_G} < F_i \\ c_{i,j} + r\left(c_{i,j} - Ig_{Gj}\right) & ; \text{ else} \end{cases} \quad (18)$$

for $i = \lfloor N/2 \rfloor + 1, \lfloor N/2 \rfloor + 2, ..., N$ and

$j = 1,2,...,M$.

The updated position of all coatis is estimated according to equation (19), where, C_i^{P1} refers to the new position of coati, $\lfloor . \rfloor$ refers to a ground function and Int refers to an integer.

$$C_i = \begin{cases} C_i^{P1}, & F_i^{P1} < F_i \\ C_i, & \text{else} \end{cases} \quad (19)$$

Improved escaping from predator's procedure: When a coati is targeted by a predator, it swiftly flees its current location. The coati's tactical movements in this scenario result in it finding a secure spot near its original position, highlighting the COA's adeptness in exploiting local search opportunities. The escaping strategy of coati towards the random position is estimated according to equations (20) and (21).

$$L_{b_j}^{\ local} = \frac{L_{b_j}}{t}; \; U_{b_j}^{\ local} = \frac{U_{b_j}}{t} \quad (20)$$

$$C_i^{P2} : c_{i,j}^{P2} = c_{i,j} + (1-2r)\left(L_{b_j}^{\ local} + r.\left(U_{b_j}^{\ local} - L_{b_j}^{\ local}\right)\right) \quad (21)$$

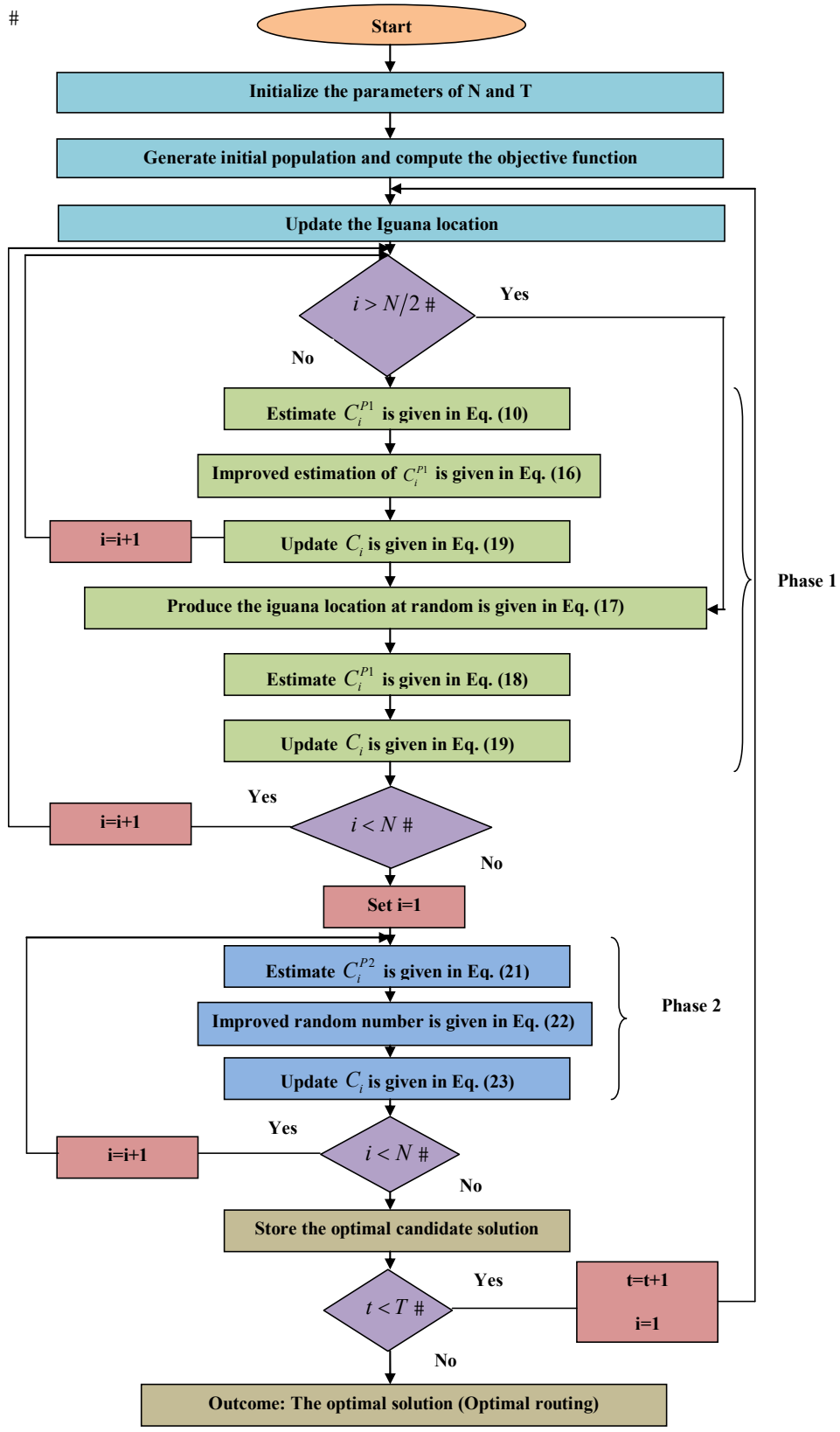
The above equation (21) is improved, in which the randomly generated number is modified to obtain an efficient position (i.e., escaping from predators and find random position) by estimating tanh chaotic map (Chaves et al., 2016) is expressed according to equation (22). Here, $e = 2/\tanh(r)$ and $y > 0, when\ b = 0$.

$$f(r) = \begin{cases} e * \tanh\left(y.(r+1) - 1\right) & ; r < 0 \\ (-1)^b.\left(e * \tanh\left(-y(r-1)\right) - 1\right) & ; r \geq 0 \end{cases} \quad (22)$$

The updated position of coati to enrich the objective function is estimated according to equation (23), where, C_i^{P2} refers to new position of coati in the exploitation stage.

$$C_i = \begin{cases} C_i^{P2}, & F_i^{P2} < F_i \\ C_i, & \text{else} \end{cases} \quad (23)$$

Figure2 Flow chart of proposed hybrid optimisation BwACO (see online version for colours)



3.3 Traffic management and congestion control

The traffic management unit (Habelalmateen et al., 2022) offers the exact route plan to efficiently transmit the data packets. The major responsibility of this unit is to manage the entire network. Moreover, this unit gathers certain following information on the density of vehicles at distinct places, the position of the vehicle and their destination place. Also, the traffic is managed by the cluster head. As the vehicles are mobile nodes, the following two considerations take place namely, (i) vehicles which are leaving the cluster and (ii) vehicles which are joining the cluster. While leaving and joining the cluster, the cluster head is also gets updated using the FCM technique as per equations (1) and (2).

Vehicles which are leaving the cluster: VANET represents a dynamically shifting topology, in which the vehicles in clusters often get the replacement in accordance with the mobility of the vehicle. When the cluster member (vehicles) desires to leave the current cluster, the specific vehicle transmits a message to the nearby cluster head.

Vehicles which are joining the cluster: The new cluster head selected as per the FCM technique sends the request message to the cluster members, which are available at the moment. Conversely, the cluster member additionally sends the request message to join the new cluster if it is necessary. According to these two constraints, the traffic and congestion control process is maintained.

As illustrated in Figure 3, consider three clusters A, B and C. In cluster A, '10' is assumed as cluster head (vehicle) and (1, 2, 4) are considered to be cluster members (vehicles); In cluster B, '9' is assumed as cluster head and (3, 8, 11) are considered to be cluster members and in cluster C, '6' is the cluster head and (5, 7) are the cluster members. These are the original representations of vehicles before leaving and joining.

In cluster A, cluster member '4' moves towards the further cluster; then cluster head '10' sends the request message to cluster head '9' (i.e., cluster member '4' leaving cluster A). The cluster head '9' of cluster B accepts the request message and the cluster member '4' joins cluster B. Thus, cluster B have new members and simultaneously, the cluster head is also varied. The new formation of the cluster after the vehicle joins the cluster is illustrated in Figure 4.

Figure 3 Vehicles before leaving the cluster (see online version for colours)

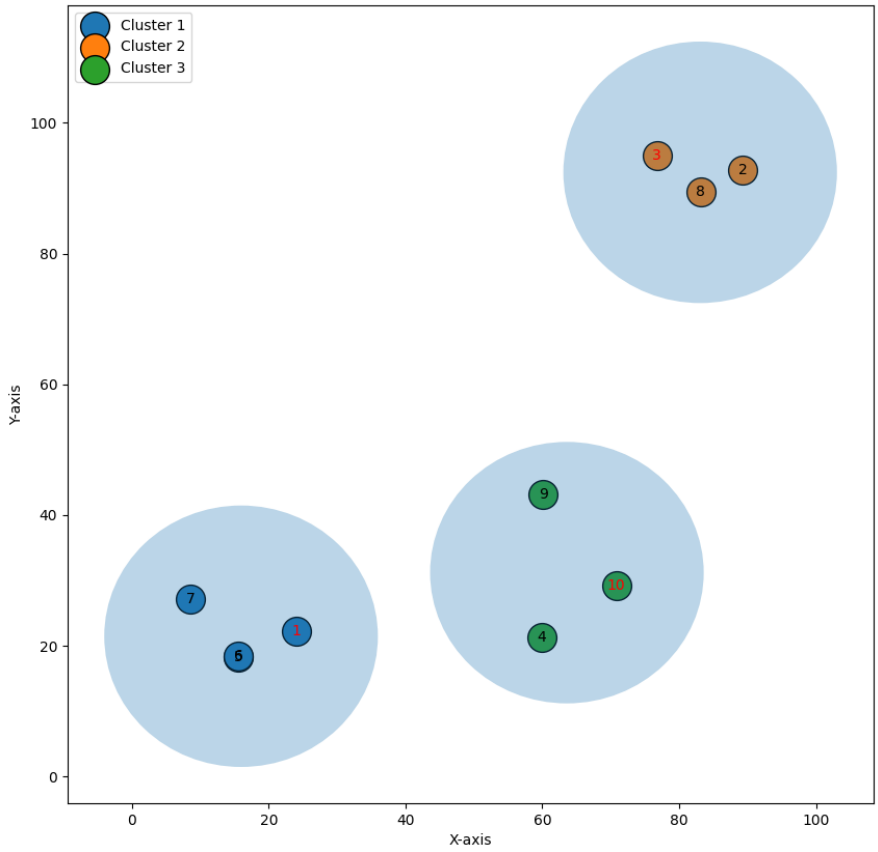
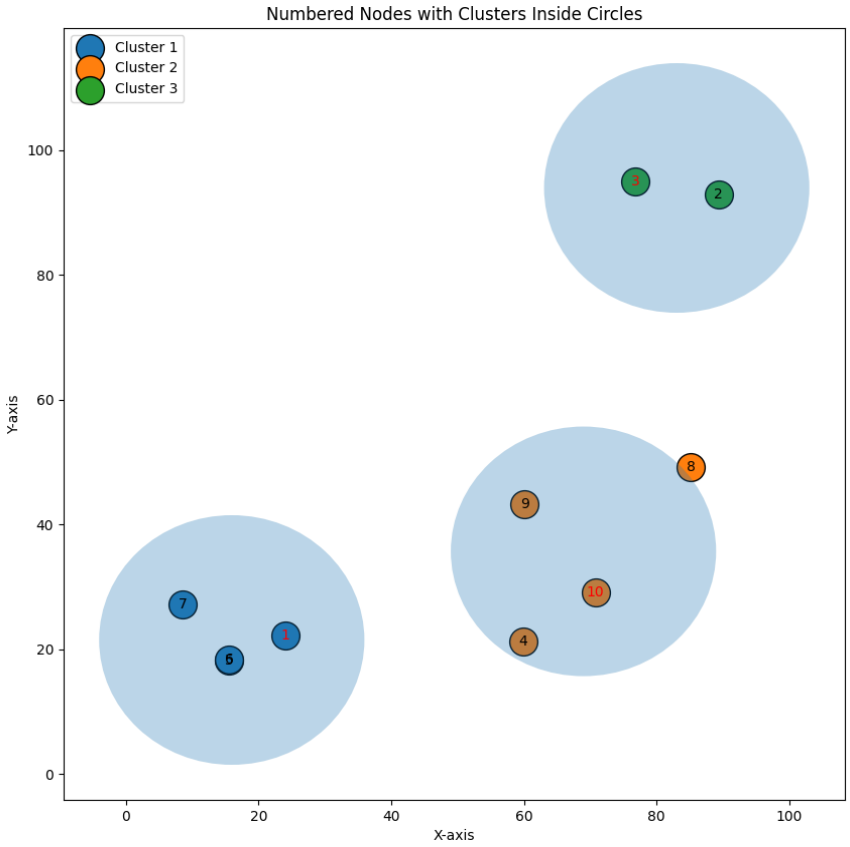


Figure 4 New formation of the clusters after a vehicle joins a cluster (see online version for colours)



3.4 Reliable retransmission

Reliable retransmission is the process of delivering reliable communication from sender to receiver over an unreliable network framework. To enhance the performance of retransmission the Packet Loss Ratio (PLR) approach is employed during data transmission. Moreover, it improves the reliability of data delivery in the presence of packet corruption or loss. A Selective Acknowledgement (SACK) enables the receiver to acknowledge various non-continuous sets of delivered messages rather than deploying last-in order-wise acknowledging packer received. Additionally, it allows the sender to retransmit the damaged or missing packets by lowering the unnecessary retransmission. Thus, it enhances the network efficiently. The approaches that are followed by the sender and receiver are as follows:

Sender side: The sender has a list of packets and keeps track of which packets to be sent sequentially. The sender assigns the sequence number for the packet to be sent. When the packet is transmitting to the receiver side, mark it as 'sent'. Finally, send the next packet based on the sequence number and return the packet data.

Receiver side: The receiver keeps track of receiving the expected sequence number of the incoming packet. If the received packet matches the expected sequence number then it generates an acknowledgement to the packet.

For reliable retransmission, the PLR is estimated once the packet is obtained at the receiver side. The PLR is estimated according to equation (24). Here, $PDR = Rp/P_n$, where, Rp refers to the received packet and P_n refers to the total number of packets.

$$PLR = 1 - PDR \tag{24}$$

Also, once the packet is obtained at the receiver side, the packet will be dropped according to packet loss probability. By employing the rate of PLR, the packet is validated for each iteration whether the packet is lost or not. If the receiver successfully receives the packet, it sends an acknowledgement to the receiver side; otherwise, the process is iterated. Further, the iteration is continued until the sender sends all the packets.

3.4.1 Pseudo-code of reliable retransmission

Algorithm 1: Reliable retransmission

Initialise the sender node, and receiver node.
  If PLR<Loss Probability
    Send packet
    If packet ≠ Null
      Generate acknowledge
      If acknowledged packet ≠ Null
        Generate SACK
  else
    Packet dropped
  $Itr = Itr + 1$
  end
Return

4 Results and discussion

4.1 Simulation Procedure

The developed Enhanced Trust-based Protocol for VANETs was implemented in Python. Also, the Python version was 'Python 3.7' and the processor utilised was '11th Gen Intel(IR) Core(TM) i5-1135G7 @ 2.40GHz 2.42 GHz' as well as the installed RAM size was '16.0 GB (15.7 GB usable)'. Table 3 represents the simulation parameters.

4.2 Performance analysis

The evaluation of BWACO and traditional schemes was analysed with regard to delay, PLR, trust, link quality, energy and distance. Further, the BWACO was compared with state-of-the-art methods, like, HRP (Sataraddi and Kakkasageri, 2020) and TACRP (Habelalmateen et al., 2022). Furthermore, Figures 5(a) and 5(b) showed the simulation setup for the nodes 100 and 200.

Table 3 Simulation parameters

S. No.	*Parameters*
1.	*x*= 100 *y* = 100
2.	# *x* and *y* coordinates of sink/Base Station sink_x = *x* * 0.5
3.	sink_y = *y* * 0.5 sinkE = 100 # Energy of sink
4.	# # Number of Nodes in the field
5.	# *n* = 100
6.	# Optimal Election Probability of a node to become cluster head *p*: float = 0.1
7.	# Initial Energy Eo: float = 0.5

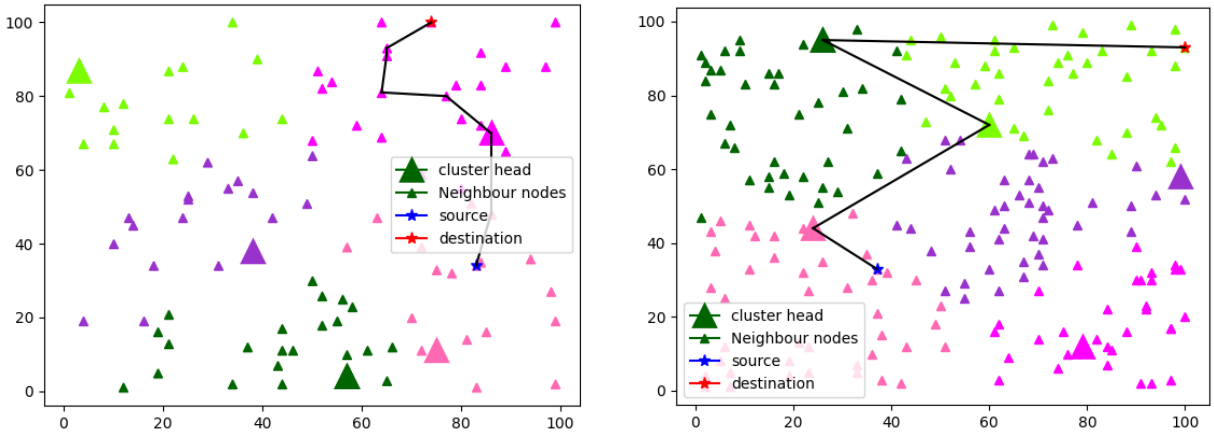
8.	# ETX = Energy dissipated in Transmission, ERX = in Receive
	Eelec: float = 50 * 0.000000001
	ETX: float = 50 * 0.000000001
	ERX: float = 50 * 0.0000000001
	
	# Transmit Amplifier types
	Efs: float = 10e-12
	Emp: float = 0.0013 * 0.000000000001
	
	# Data Aggregation Energy
	EDA: float = 5 * 0.000000001
	h = 100 # Hard Threshold H(t)
	s = 2 # Soft threshold S(t)
	sv = 0 # previously Sensed Value S(v)
	
	# temperature range
	tempi: float = 5
	tempf: float = 200
	
	# Computation of do
	do: float = sqrt(Efs / Emp)
	
	# Run Time Parameters
	# maximum number of rounds
	rmax = 2000
	# Data packet size
	data_packet_len = 4000

Table 3 Simulation parameters (continued)

S. No.	*Parameters*

	# Radio Range
	RR: float = 0.5 * x * sqrt(2)
	
	# Values for Heterogeneity
	# Percentage of nodes than are advanced
	m = 0.1
	# alpha
	alp = 1
	beta = 0.3

Figure 5 Simulation setup for VANET network (a) 100 Nodes and (b) 200 Nodes (see online version for colours)

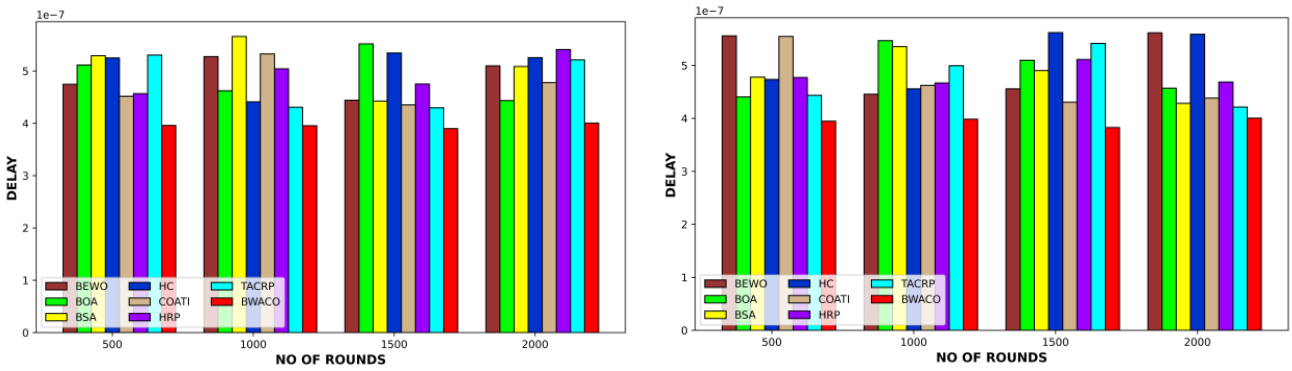


(a) (b)

4.3 Delay analysis

The delay assessment on BWACO over BEWO, BOA, BSA, HC, COATI, HRP (Sataraddi and Kakkasageri, 2020) and TACRP (Habelalmateen et al., 2022) for optimal routing under the nodes 100 and 200 is depicted in Figures 6(a) and 6(b). It is also examined for a variable number of rounds (500–2000). Similarly, the BWACO recorded lower delay values in both nodes. In particular, for the round 1500, the BWACO offered a lower delay value of $3.634\times1e^{-7}$, whilst the traditional schemes acquired maximal delay ratings, notably, BEWO=$4.572\times1e^{-7}$, BOA=$4.916\times1e^{-7}$, BSA=$4.735\times1e^{-7}$, HC=$5.829\times1e^{-7}$, COATI=$3.914\times1e^{-7}$, HRP (Sataraddi and Kakkasageri, 2020) =$4.871\times1e^{-7}$ and TACRP (Zhou and Yang, 2019) =$5.412\times1e^{-7}$, correspondingly. Hence, the BWACO employed the hybrid optimisation strategy to ensure optimal routing and maintain stable performance while minimising delay values.

Figure 6 Delay assessment on BWACO and conventional schemes (a) 100 Nodes and (b) 200 Nodes (see online version for colours)



(a) (b)

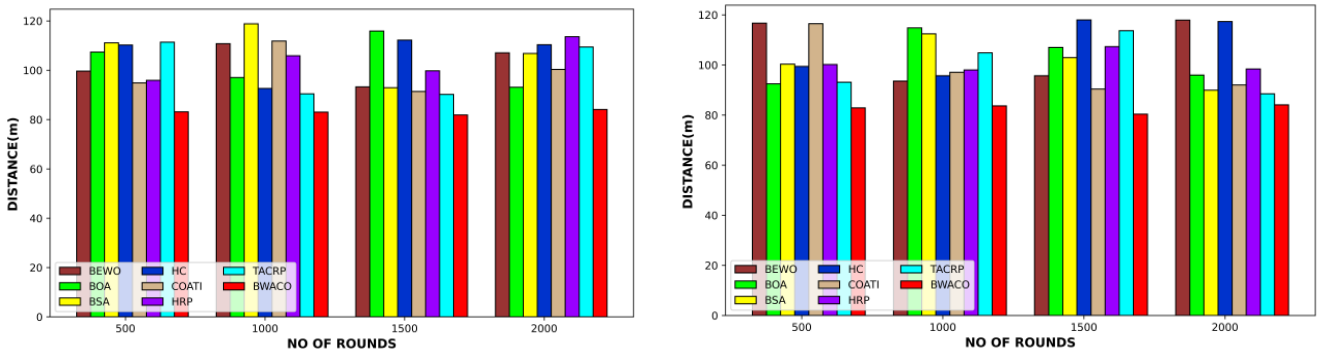
4.4 Distance analysis

Figures 7(a) and 7(b) explain the distance evaluation on BWACO is compared with BEWO, BOA, BSA, HC, COATI, HRP (Sataraddi and Kakkasageri, 2020) and TACRP (Habelalmateen et al., 2022) for computing trust in VANET with enhanced processes. Further, the distance value ought to be lesser for optimal routing VANET framework. Mainly, for node 100, the minimal distance attained using the BWACO approach is 79 m at the round 500, meanwhile, the BEWO is 99 m, BOA is 108 m, BSA is 113 m, HC is 110 m, COATI is 94 m, HRP (Sataraddi and Kakkasageri, 2020) is 95 m and TACRP (Habelalmateen et al., 2022) is 115 m, correspondingly. In nearly every round, the BWACO approach obtained lower distance values for the opposite node. As a result, it can be said that the BWACO method, which selects the best routing in VANETs, is adept at offering very efficient solutions with smaller distance values.

4.5 Energy analysis

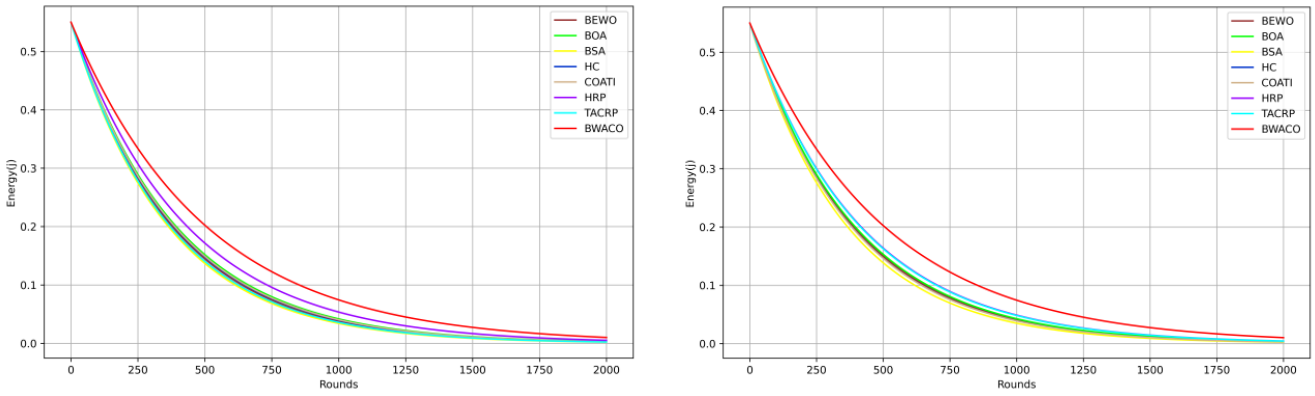
The energy evaluation on BWACO over BEWO, BOA, BSA, HC, COATI, HRP (Sataraddi and Kakkasageri, 2020) and TACRP (Habelalmateen et al., 2022) for optimal routing is described in Figures 8(a) and 8(b). At the initial (0^{th}) round, the BWACO and conventional strategies yielded lesser energy ratings, yet as the round improved the energy value was enhanced. Nonetheless, the BWACO accomplished greater energy values from the initial to the final rounds. Considering the Figure 8(b), at around 2000, the BWACO obtained maximal energy values than traditional schemes, such as BEWO, BOA, BSA, HC, COATI, HRP (Sataradd and Kakkasageri, 2020) and TACRP (Habelalmateen et al., 2022), correspondingly. The selection of optimal routing in the VANET framework is facilitated through the hybrid optimisation method (combining COATI and BWO). This enhances the energy efficiency of the BWACO scheme.

Figure 7 Distance assessment on BWACO and conventional schemes (a) 100 Nodes and (b) 200 Nodes (see online version for colours)



(a) (b)

Figure 8 Energy assessment on BWACO and conventional schemes (a) 100 Nodes and (b) 200 Nodes (see online version for colours)



(a) (b)

4.6 Analysis of link quality

The evaluation of BWACO and traditional methods regards of link quality for optimal routing in the VANET framework is explained in Figures 9(a) and 9(b). The quality of data packets that the recipient receives is known as link quality. Here, the packet loss ratio is used to analyse the link quality. The packet loss ratio decreases as the network quality increases. Particularly, the BWACO produced a link quality of 0.958 at the round 2000, although the BEWO (0.637), BOA (0.594), BSA (0.789), HC (0.613), COATI (0.648), HRP (Sataraddi and Kakkasageri, 2020) (0.652) and TACRP (Habelalmateen et al., 2022) (0.661), correspondingly. The thorough evaluation of link quality highlights the suitability of the BWACO strategy for identifying the most suitable routing in the VANET method.

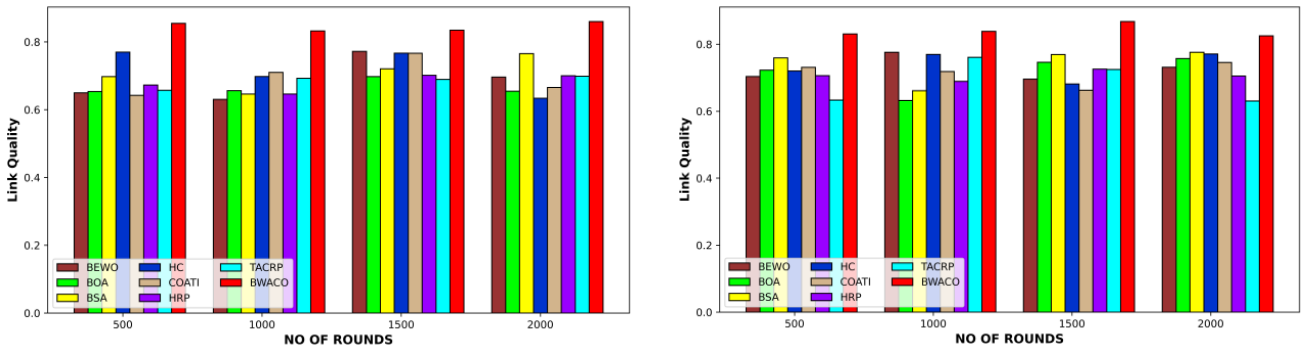
4.7 PLR analysis after reliable retransmission

The PLR evaluation on BWACO over BEWO, BOA, BSA, HC, COATI, HRP (Sataraddi and Kakkasageri, 2020) and TACRP (Habelalmateen et al., 2022) for the analysis after reliable retransmission is explained in Figures 10(a) and 10(b). Here, the BWACO gained minimal PLR as well as it quickly recovered the missed packets. For the node 200, the lesser PLR is obtained using the BWACO scheme is 0.175 (Round=1500), while the BEWO (0.269), BOA (0.248), BSA (0.231), HC (0.238), COATI (0.257), HRP (Sataraddi and Kakkasageri, 2020) (0.283) and TACRP (Habelalmateen et al., 2022) (0.379), correspondingly. As a result, the results show how much the BWACO technique improves PLR (after retransmission) efficiency when it comes to VANET routing.

4.8 PLR analysis before reliable retransmission

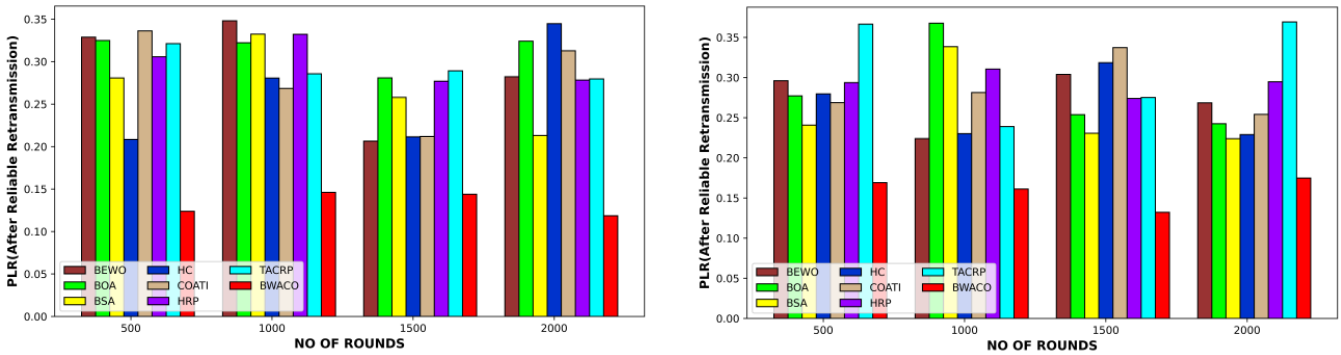
The PLR evaluation on BWACO is contrasted with BEWO, BOA, BSA, HC, COATI, HRP (Sataraddi and Kakkasageri, 2020) and TACRP (Habelalmateen et al., 2022) before reliable retransmission is exposed in Figures 11(a) and 11(b). While assessing both figures, the BWACO reduced the PLR as well as it reduced the retransmission. Mainly, for node 100, the BWACO holds the PLR of 0.124 in round 2000, even though the BEWO, BOA, BSA, HC, COATI, HRP (Sataraddi and Kakkasageri, 2020) and TACRP (Habelalmateen et al., 2022) scored minimised PLR ratings. In a similar vein, the BWACO produced lower PLR rates than the conventional methods for node 200 in every round.

Figure 9 Link quality assessment on BWACO and conventional schemes (a) 100 Nodes and (b) 200 Nodes (see online version for colours)



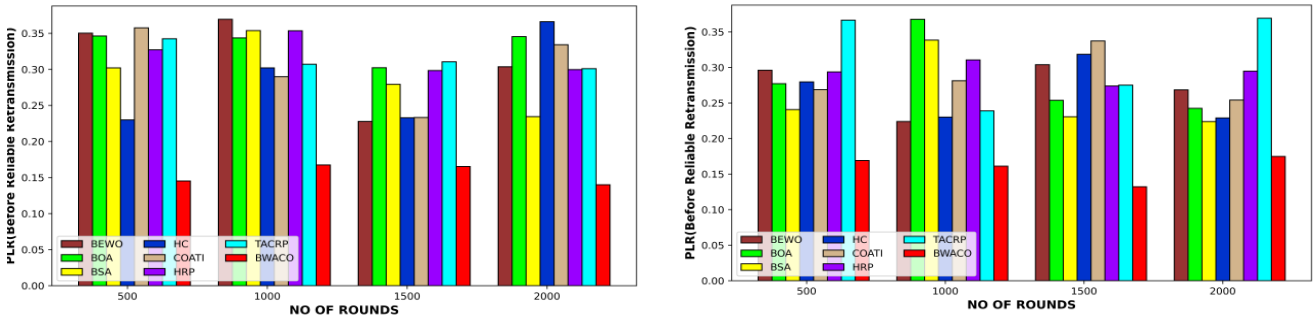
(a) (b)

Figure 10 PLR assessment on BWACO and conventional schemes for after reliable retransmission (a) 100 Nodes and (b) 200 Nodes (see online version for colours)



(a) (b)

Figure 11 PLR assessment on BWACO and traditional techniques before reliable retransmission (a) 100 Nodes and (b) 200 Nodes (see online version for colours)



(a) (b)

4.9 Analysis of trust

The trust assessment on BWACO and the conventional methodologies for optimal routing under nodes 100 and 200 are shown in Figures 12(a) and 12(b). Moreover, the BWACO is contrasted with the traditional schemes, like, BEWO, BOA, BSA, HC, COATI, HRP (Sataraddi and Kakkasageri, 2020) and TACRP (Habelalmateen et al., 2022). Further, the trust rate of the BWACO methodology is 0.093 (Round=1500), whilst the prior methods recorded lower trust rates, including, BEWO=0.073, BOA=0.075, BSA=0.067, HC=0.069, COATI=0.070, HRP (Sataraddi and Kakkasageri, 2020) =0.068 and TACRP (Habelalmateen et al., 2022) =0.067, correspondingly.

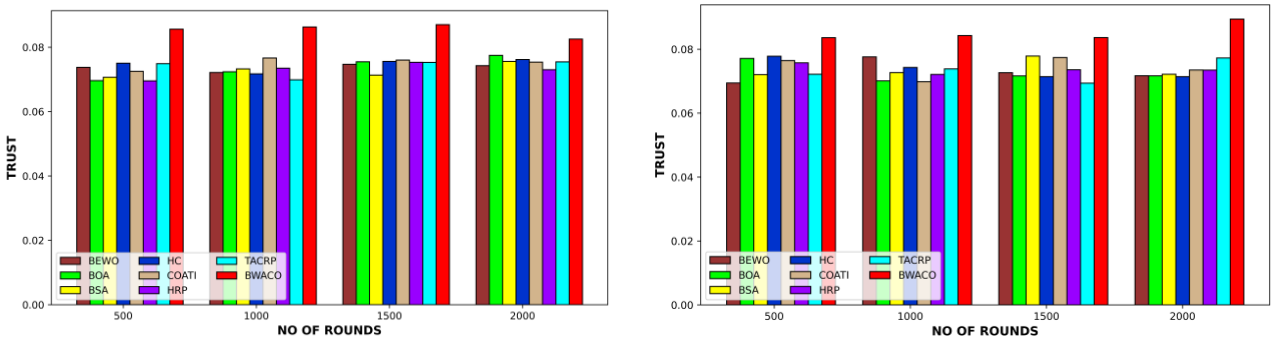
4.10 Convergence analysis

The convergence study on BWACO is compared with BEWO, BOA, BSA, HC and COATI for computing trust in VANET with enhanced processes at the nodes100 and 200 and is presented in Figures 13(a) and 13(b). In addition, a faster convergence of the cost value is required for the model to function effectively. Both the BWACO and conventional approaches received greater fitness ratings in the first iteration; however, as the iterations went on, the value of fitness dropped. Still, the BWACO scored minimal fitness ratings. Mainly, the BWACO obtained the fitness value of 1.141 at the 25th iteration, whereas the BEWO is 1.218, BOA is 1.517, BSA is 1.349, HC is 1.327 and COATI is 1.197, respectively. The incorporation of a hybrid optimisation strategy (COATI and BWO) is a primary factor in the BWACO method's ability to attain quicker convergence.

4.11 Statistical evaluationof fitness and mobility

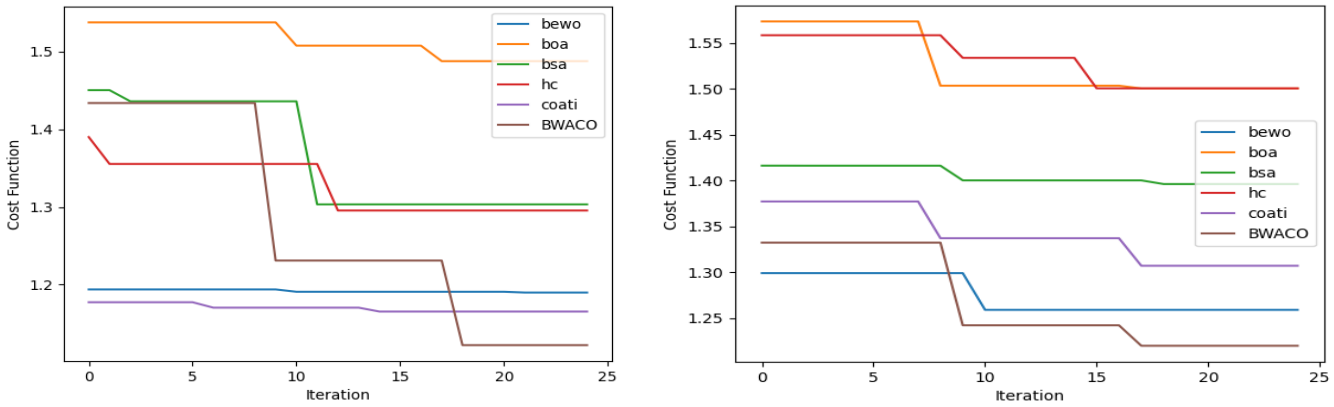
The statistical study on BWACO is contradicted by BEWO, BOA, BSA, HC, COATI, HRP (Sataraddi and Kakkasageri, 2020) and TACRP (Habelalmateen et al., 2022) with regard to fitness and mobility for computing trust in VANET with enhanced processes are summarised in Tables 4 to 7. Further, the BWACO achieved the lowest fitness value of 1.122 (see Table 4) under the lesser values, meanwhile, the BEWO is 1.190, BOA is 1.488, BSA is 1.303, HC is 1.295 and COATI is 1.165, respectively.

Figure 12 Trust assessment on BWACO and conventional schemes (a) 100 Nodes and (b) 200 Nodes (see online version for colours)



(a) (b)

Figure 13 Convergence analysis on BWACO and conventional schemes (a) 100 Nodes and (b) 200 Nodes (see online version for colours)



(a) (b)

Table 4 Statistical analysis of fitness for 100 nodes

Statistical metrics	*BEWO*	*BOA*	*BSA*	*HC*	*COATI*	*BWACO*
Mean	1.192	1.513	1.363	1.326	1.170	1.273
Standard deviation	0.002	0.021	0.067	0.032	0.005	0.128
Maximum	1.194	1.538	1.450	1.390	1.177	1.434
Median	1.191	1.508	1.303	1.295	1.170	1.231
Minimum	1.190	1.488	1.303	1.295	1.165	1.122

Table 5 Statistical analysis of Fitness for 200 nodes

Statistical metrics	*BEWO*	*BOA*	*BSA*	*HC*	*COATI*	*BWACO*
Mean	1.275	1.525	1.405	1.529	1.340	1.268
Standard deviation	0.020	0.033	0.009	0.025	0.028	0.049
Maximum	1.299	1.573	1.416	1.558	1.377	1.332
Median	1.259	1.503	1.400	1.534	1.337	1.242
Minimum	1.259	1.500	1.396	1.500	1.307	1.220

Additionally, the statistical evaluation of the BWACO and existing techniques with regard to mobility is tabulated in Tables 6 and 7. In particular, the greatest mobility offered using the BWACO approach is –146.386 at the median statistical metric, though the previous techniques obtained minimal mobility ratings, such as BEWO= –174.033, BOA= –174.053, BSA= –173.928, HC= –174.058, COATI= –174.076, HRP (Sataraddi and Kakkasageri, 2020) =–174.009 and –174.116, correspondingly.

Table 6 Statistical analysis of mobility for 100 nodes

Methods	*Minimum*	*Mean*	*Standard Deviation*	*Maximum*	*Median*
BEWO	–178	–174.017	2.317796	–170	–174.033
BOA	–177.995	–174.025	2.314789	–170.002	–174.053
BSA	–177.992	–173.994	2.321888	–170.004	–173.928
HC	–177.987	–174.009	2.322905	–170.001	–174.058
COATI	–178	–174.003	2.290173	–170.002	–174.076
HRP [21]	–177.995	–173.955	2.290179	–170.004	–174.009
TACRP [22]	–177.999	–174.062	2.308064	–170.001	–174.116
BWACO	–168.972	–146.167	13.2856	–123.039	–146.386

Table 7 Statistical analysis of mobility for 200 nodes

Methods	*Minimum*	*Mean*	*Standard Deviation*	*Maximum*	*Median*
BEWO	–177.993	–173.981	2.276	–170.002	–173.914
BOA	–178.000	–174.060	2.362	–170.002	–174.118
BSA	–177.997	–174.026	2.273	–170.000	–174.003
HC	–177.996	–174.034	2.289	–170.020	–174.054
COATI	–177.993	–173.994	2.296	–170.001	–173.997
HRP (Sataraddi and Kakkasageri, 2020)	–177.998	–174.002	2.318	–170.001	–173.976
TACRP (Habelalmateen et al., 2022)	–177.999	–173.923	2.291	–170.001	–173.873
BWACO	–168.986	–145.890	13.239	–123.027	–146.170

5 Conclusion

The three phases below were used in the construction of this upgraded trust-based protocol that is being proposed: cluster head selection and optimal routing were used in the VANET routing procedure; the FCM method was employed to select the cluster head and proposed an innovative optimisation strategy called Beluga whale Assisted in Coati Optimisation (BwACO) algorithm for choosing optimal routing; subsequently, the traffic management and congestion control process was performed under the consideration of a vehicle which is leaving the cluster and a vehicle which is joining the cluster. Finally, a reliable transmission process was performed by considering the following stages like packet transmission, acknowledgement, retransmission and maximum retransmission attempts. The BWACO scheme yields a lesser PLR of 0.175 (Round=1500), but the BEWO (0.269), BOA (0.248), BSA (0.231), HC (0.238), COATI (0.257), HRP (0.283) and TACRP (0.379) yield, respectively, higher PLRs. In order to establish more effective data routing paths based on reinforcement learning approach, we will incorporate additional parameters in the future, taking into account the Internet of Things environment, such as dynamic traffic load or connection breakage.

References

Abassi, R., Douss, A.B.C. and Sauveron, D. (2020) 'TSME: a trust-based security scheme for message exchange in vehicular Ad hoc networks', *Human Centric Computing and Information Sciences*, Vol. 10, No. 43. Doi: 10.1186/s13673-020-00248-4.

Abdollah, S. and Zarei, M. (2021) 'A traffic-centric fuzzy approach for solving the starvation problem of cooperative awareness messages in vehicular ad hoc networks', *International Journal of Communication Systems*, Vol. 34, No. 18. Doi: 10.1002/dac.4999.

Ahmad, F., Franqueira, V.N.L. and Adnane, A. (2018) 'TEAM: a trust evaluation and management framework in context-enabled vehicular ad-hoc networks', *IEEE Access*, Vol. 6, pp.28643–28660. Doi: 10.1109/ACCESS.2018.2837887.

Ahmed, S., Rehman, M.U., Ishtiaq, A., Khan, S., Ali, A. and Begum, S. (2018) 'VANSec: attack-resistant VANET security algorithm in terms of trust computation error and normalized routing overhead', *Journal of Sensors*. Doi: 10.1155/2018/6576841.

Azizi, M. and Shokrollahi, S. (2024) 'RTRV: an RSU-assisted trust-based routing protocol for VANETs', *Ad Hoc Networks*, Vol. 154. Doi: 10.1016/j.adhoc.2023.103387.

Azzoug, Y. and Boukra, A. (2024) 'Improved junction-based routing for VANETs using a bio-inspired route stability approach', *Ad Hoc Networks*, Vol. 153. Doi: 10.1016/j.adhoc.2023.103346.

Chaves, D.P.B., Souza, C.E.C. and Pimentel, C. (2016) 'A smooth chaotic map with parameterized shape and symmetry', *EURASIP Journal on Advances in Signal*. Doi: 10.1155/2018/6576841.

Chukwuocha, C., Thulasiraman, P. and Thulasiram, R.K. (2021) 'Trust and scalable blockchain-based message exchanging scheme on VANET', *Peer-to-Peer Networking Applications*, Vol. 14, pp.3092–3109. Doi: 10.1007/s12083-021-01164-9.

Dehghani, M., Montazeri, Z., Trojovská, E. and Trojovský, P. (2023) 'Coati optimization algorithm: a new bio-inspired metaheuristic algorithm for solving optimization problems', *Knowledge-Based Systems*, Vol. 259. Doi: 10.1016/j.knosys.2022.110011.

Gazdar, T., Alboqomi, O. and Munshi, A. (2022) 'A decentralized blockchain-based trust management framework for vehicular ad hoc networks', *Smart Cities*, Vol. 5, pp.348–363. Doi: 10.3390/smartcities5010020.

Gazdar, T., Belghith, A. and Abutair, H. (2018) 'An enhanced distributed trust computing protocol for VANETs', *IEEE Access*, Vol. 6, pp.380–392. Doi: 10.1109/ACCESS.2017.2765303.

Ghajar, F.G., Sratakhti, J.S. and Sikora, A. (2021) 'SBTMS: scalable blockchain trust management system for VANET', *Applied Sciences*, Vol. 11. Doi: 10.3390/app1124119.

Habelalmateen, M.I., Ahmed, A.J., Abbas, A.H. and Rashid, S.A. (2022) 'TACRP: traffic-aware clustering-based routing protocol for vehicular ad-hoc networks', *Designs*, Vol. 6, No. 5. Doi: 10.3390/designs6050089.

Hasrouny, H., Samhat, A.E., Bassil, C. and Laouiti, A. (2019) 'Trust model for secure group leader-based communications in VANET', *Wireless Networks*, Vol. 25, pp.4639–4661. Doi: 10.1007/s11276-018-1756-6.

Hemmati, A., Zarei, M. and Rahmani, A.M. (2024) 'A systematic review of congestion control in internet of vehicles and vehicular ad hoc networks: techniques, challenges, and open issues', *International Journal of Communication Systems*, Vol. 37, No. 1. Doi: 10.1002/dac.5625.

Inedjaren, Y., Maachaoui, M., Zeddini, B. and Barbot, J-P. (2021) 'Blockchain-based distributed management system for trust in VANET', *Vehicular Communications*, Vol. 30. Doi: 10.1016/j.vehcom.2021.100350.

Kadam, M.V., Vaze, V.M. and Todmal, S.R. (2023) 'TACR: trust aware clustering-based routing for secure and reliable VANET communications', *Wireless Personal Communications*, Vol. 132, No. 1, pp.305–328.

Kaur, G. and Kakkar, D. (2022) 'Hybrid optimization enabled trust-based secure routing with deep learning-based attack detection in VANET', *Ad Hoc Networks*, Vol. 136. Doi: 10.1016/j.adhoc.2022.102961.

Khan, A.S., Balan, K., Javed, Y., Tarmizi, S. and Abdullah, J. (2019) 'Secure trust-based blockchain architecture to prevent attacks in VANET', *Sensors*, Vol. 19. Doi: 10.3390/s19224954.

Kudva, S., Badsha, S., Sengupta, S., La, H., Khalil, I. and Atiquzzaman, M. (2021) 'A scalable blockchain based trust management in VANET routing protocol', *Journal of Parallel and Distributed Computing*, Vol. 152, pp.144–156. Doi: 10.1016/j.jpdc.2021.02.024.

Li, B., Liang, R., Zhu, D., Chen, W. and Lin, Q. (2021) 'Blockchain-based trust management model for location privacy preserving in VANET', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 22, No. 6, pp.3765–3775. Doi: 10.1109/TITS.2020.3035869.

Liu, X., Huang, H., Xiao, F. and Ma, Z. (2020) 'A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs', *IEEE Internet of Things Journal*, Vol. 7, No. 5, pp.4101–4112. Doi: 10.1109/JIOT.2019.2957421.

Malik, N., Nanda, P., He, X. and Liu, R.P. (2020) 'Vehicular networks with security and trust management solutions: proposed secured message exchange via blockchain technology', *Wireless Network*, Vol. 26, pp.4207–4226. Doi: 10.1007/s11276-020-02325-z.

Poongodi, M., Hamdi, M., Sharma, A., Ma, M. and Singh, P.K. (2019) 'DDoS detection mechanism using trust-based evaluation system in VANET', *IEEE Access*, Vol. 7, pp.183532–183544. Doi: 10.1109/ACCESS.2019.2960367.

Rehman, A. et al. (2022) 'CTMF: context-aware trust management framework for internet of vehicles, *IEEE Access*, Vol. 10, pp.73685–73701. Doi: 10.1109/ACCESS.2022.3189349.

Sataraddi, M.J. and Kakkasageri, M.S. (2020) 'Hybrid routing protocol for VANETs: delay and trust based approach', *Journal of High Speed Networks*, Vol. 1, pp.1–16. Doi: 10.3233/JHS-200644.

Souri, A. (2022) 'Artificial intelligence mechanisms for management of QoS-aware connectivity in internet of vehicles', *Journal of High Speed Networks*, pp.1–10.

Tangade, S., Manvi, S.S. and Lorenz, P. (2020) 'Trust management scheme based on hybrid cryptography for secure communications in VANETs', *IEEE Transactions on Vehicular Technology*, Vol. 69, No. 5, pp.5232–5243. Doi: 10.1109/TVT.2020.2981127.

Yan, X., Gu, X., Wang, J., Wan, J. and Chen, L. (2021) 'A kind of event trust model for VANET based on statistical method', *Wireless Personal Communication*, Vol. 118, pp.489–503. Doi: 10.1007/s11277-020-08027-1.

Zhang, J., Zheng, K., Zhang, D. and Yan, B. (2020) 'AATMS: an anti-attack trust management scheme in VANET', *IEEE Access*, Vol. 8, pp.21077–21090. Doi: 10.1109/ACCESS.2020.2966747.

Zhong, C., Li, G. and Meng, Z. (2022) 'Beluga whale optimization: a novel nature-inspired metaheuristic algorithm', *Knowledge-Based Systems*, Vol. 251. Doi: 10.1016/j.knosys.2022.109215.

Zhou, K. and Yang, S. (2019) 'Effect of cluster size distribution on clustering: a comparative study of k-means and fuzzy c-means clustering', *Pattern Analysis and Applications*. Doi: 10.1007/s10044-019-00783-6.