Human-Centric Intelligent Systems (2024) 4:25–52
https://doi.org/10.1007/s44230-023-00059-7

RESEARCH ARTICLE

An Enhanced Location-Aided Ant Colony Routing for Secure Communication in Vehicular Ad Hoc Networks

Raghu Ramamoorthy[1]

Received: 2 October 2023 / Accepted: 13 December 2023 / Published online: 10 January 2024

Abstract

The dynamic characteristics of vehicular ad hoc networks (VANETs) demand reliable and secure communication over wireless media. However, there are significant contradictions in autonomous vehicular systems related to security and privacy. Furthermore, VANETs require seamless data transmission to exchange time-critical data about accidents and traffic. Therefore, VANETs require secure seamless data transmission mechanisms to provide secure reliable communication without communication interruption to exchange time-critical data between vehicles. This paper proposes an Enhanced Location-Aided Ant colony Routing (ELAACR) for VANETs to achieve seamless secure data transmission. The proposed ELAACR is a two-fold scheme in which Phase 1 implements Location-Aided Key Management (LAKM) and Phase 2 implements Ant Colony Routing (ACR). An ACR combined with an LAKM pattern for offering secure and reliable communication. The LAKM scheme works based on the group signature concept to construct a secure network, and an ACR is used to find an efficient secure shortest path for seamless data transmission. The proposed work is simulated in Network Simulator (NS 2.35). By using an efficient and secure shortest path with secure seamless data transmission, the proposed ELAACR achieves an average throughput (T) of 640 Kbps, packet loss rate (PLR) of 0.018%, packet delivery ratio (PDR) of 98.5%, overhead (OH) of 0.157%, and 0.16 s end-to-end delay (EED) compared to Enhanced Hybrid Ant Colony Optimization Routing Protocol (EHACORP) and Fuzzy Based Ant Colony Optimization (F-ANT). The simulation results show that the proposed ELAACR registers better performance in all aspects compared to the existing EHACORP and F-ANT.

Keywords Routing · Shortest path · Ant colony routing · Efficient path · Secure communication

Abbreviations

ACO	Ant colony optimization
ACR	Ant colony routing
AKANT	Acknowledgment ANT
CAS	Certificate less aggregate signature
CBR	Constant bit rate
D	Destination
DBF	Direction-based forwarding
DCAs	Data carry ants
DLAR	Direction-based location-aided routing
DSRC	Dedicated short-range communication
eACO	Enhanced ant colony optimization
EBIRA	Enhanced bio-inspired routing algorithm
EED	End-to-end delay
EHACORP	Enhanced hybrid ant colony optimization routing protocol
ELAACR	Enhanced location-aided ant colony routing
F-ANT	Fuzzy-based ant colony optimization
GM	Group manager
GPS	Global positioning system
GPSR	Greedy perimeter stateless routing
GS	Group signature
ITS	Intelligent transportation systems
LAKM	Location-aided key management
LAR	Location-aided routing
LGM	Legitimate group member
MANETs	Mobile ad hoc networks
MAODV	Modified ad hoc on-demand distance vector
MATLAB	Matrix laboratory
MOVE	Mobility model generator for vehicular networks
N	Network
NRL	Normalized routing load

✉ Raghu Ramamoorthy
raghuace85@gmail.com

[1] Department of Computer Science and Engineering, The Oxford College of Engineering, Bengaluru, Karnataka 560068, India

NS2	Network simulator
OBU	On-board unit
OGM	Offline group manager
OH	Overhead
OTcl	Object tool command language
PDR	Packet delivery ratio
PLR	Packet loss rate
QoS	Quality of service
REANTs	Route explorer ants
REHANT	Route error handling ant
RMANTs	Route manage ants
RO	Routing overhead
RSP	Route selection parameter
RSUs	Road side units
S	Source
ST	Simulation time
SUMO	Simulation of urban mobility
T	Throughput
TCL	Tool command language
V	Vehicle
V2I	Vehicle to fixed unit
V2V	Vehicle to vehicle
VANETs	Vehicular ad hoc networks
XML	Extensible markup language

1 Introduction

A vehicular ad hoc network (VANET) is a network consisting of a collection of moving vehicles. VANET imports all the characteristics of mobile ad hoc networks (MANETs) with additional parameters such as high mobility, frequent route breaks, and dynamic topology. Being a sub-type of MANETs, VANETs often experience communication link breaks due to imbalances in vehicle availability. VANETs are intended to exchange various types of information between vehicles regarding traffic, entertainment, road conditions, etc. VANETs include communication frameworks such as Vehicle to Vehicle (V2V) and Vehicle to Fixed Unit (V2I) to support communication between vehicles [1]. Fig. 1 represents V2V and V2I communication in VANETs. VANET is used in Intelligent Transportation Systems (ITS). Vehicles in VANETs are fitted with a range of hardware components, including processing power, communication entities, On-Board Unit (OBU), and Global Positioning System (GPS) units. An OBU is a device that is mounted in a vehicle and used in VANETs to communicate with other OBUs and Road side units (RSUs). RSU is deployed in specific locations, like junctions and roadside areas. To communicate with the infrastructure network and vehicles, the RSU uses radio technology based on Dedicated Short-Range Communications (DSRC) [2].

The non-efficient paths can face frequent interruptions due to the high movement of vehicles on the road. The mobility, frequent changes in network layout, and wireless communication can damage the path at any time without any symptoms. Additionally, the dynamic assets of VANETs such as dynamic topology with wireless communication may generate additional problems for communication. Because of the high-impact properties of VANETs, transmitting time-oriented data over wireless channels is a hard task [3, 4]. The message routing method which is in practice for

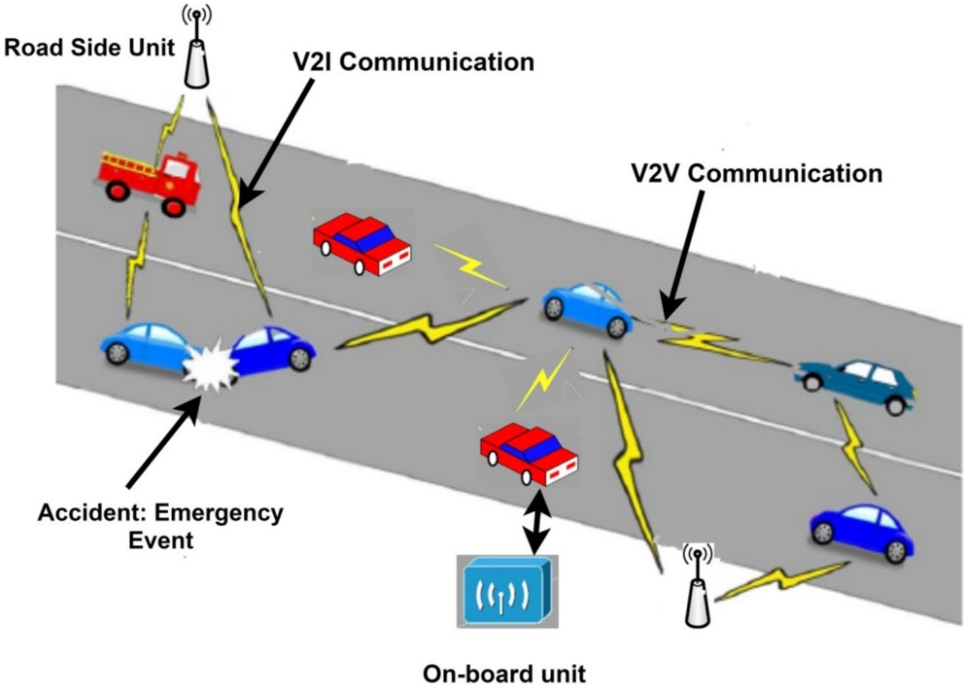


Fig. 1 V2V and V2I communication in VANETs

VANETs should cope with VANET properties. The routing approaches need to tend to offer secure communication. Intruders can attack wireless communication in terms of passive or active attacks. Passive attacks are very hard to detect. The communication in V2V or V2I should be secure to avoid intruders from listening to the traffic. The vehicles in the path should be authenticated using valid security mechanisms.

Transmission of traffic-based/confidential messages through trusted or honest vehicles provides information security. VANET is an open-source wireless communication that is more vulnerable to various security attacks. For example, an attacker may modify/create a fake road congestion message for his benefit. Vehicles receiving a modified or fake message about traffic may make a wrong decision. Therefore, vehicles must authenticate before considering message transmission. Due to high mobility, communication time is very short and vehicles must be authenticated quickly for communication [5]. Therefore, VANETs require light white authentication mechanisms, and a group signature (GS) scheme is the best choice to authenticate vehicles in a short time. A group signature scheme allows the dynamic joining/leaving of vehicles with authentication features to provide security for information. Group Admin of GS is responsible for generating certificates and issuing/revoking certificates to group vehicles. Message signing is done through certificates, which provide low computational overhead and security for messages in VANETs. The location-aided method with group signature is the best solution to offer privacy, security, and authentication for VANETs.

Henceforth loss or delay in end-to-end data communication will cause panic and accidents in road transport. The shortest path with fewer intermediate vehicles can deliver the packets related to traffic or accident information quickly. The packets should not experience any type of delay such as processing delay, transmitting delay, propagation delay, queuing delay, waiting delay, or scheduling delay [6]. With certain modifications to routing approaches the delay issues will be solved [7, 8]. Security requirements should focus on VANET to ensure data integration, security, and authentication on data. The bio-based approaches incorporate the natural behavior of insects such as ants and bees to provide solutions for various problems such as scheduling, vehicle routing, optimization, etc., From the last decade the vast amount of enhancements introduced in VANET routing approaches with bio-based approaches. The Routing method's working style is modified with bio-inspired approaches to provide seamless data transmission with the required security.

This work significantly focuses on enhancing the routing methodology with a bio-based approach such as ACR to provide seamless data transmission among vehicles. ACR has significant advantages such as adaptability, high robustness, and distributed properties. All these advantages are the backbone of ACR to use in VANETs for routing. To impose security, the location-based group signature concept was adopted with ACR. The group signature enhances the ACR with privacy, security, and data integrity with end-to-end communication. Position-oriented group signature for the VANET system not only enhances the data security in transmission but improves the throughput and packet transmission ratio [9].

Currently, the routing domain of VANET needs extensive research to propose better routing protocols or mechanisms. In this context, ELAACR is introduced to provide secure communication in VANET. ELAACR fits the current state of VANET because seamless data transmission between vehicles is a challenging task due to VANET's rich set of dynamic characteristics. ELAACR relies on a location-aware approach and an adaptive approach such as ACR to deal with VANET characteristics. The decentralized and adaptive nature of ACR is suitable for solving dynamic and challenging situations of vehicular networks.

This work primarily aims to address the below problem statements.

- The highly dynamic features of VANETs affect the reliability and security of the routing mechanism. Exchanging time-critical information about road conditions requires reliable and secure communication between vehicles/infrastructure.
- Routing concerns such as high vehicle speeds and dynamic path breaks reduce the efficiency of the routing mechanism.
- A high level of mobility causes unexpected irregular vehicle arrival/departure and general fluctuation in the VANETs network, which affects the VANETs routing strategy in a repeated path failure mode, resulting in message communication interruption.
- In this context, a secure seamless data transmission mechanism is required for the routing mechanism to provide secure reliable communication without communication interruption to exchange time-critical data between vehicles.

1.1 The Novelty and Important Contributions of This Work Are as Follows

The novelty of the proposed work lies in introducing LAKM with ACR. LAKM provides a secure network and ACR generates efficient secure channels for seamless data transmission. Furthermore, ACR pheromone models have been improved to maintain high amounts of pheromone in optimal paths. ACR's novel optimal route discovery and route-handling mechanisms are rich in providing efficient routing for VANETs.

Contributions are,

- The proposed scheme aims to determine the efficient and secure shortest path for secure seamless data transmission.
- In the proposed model, we adopt group signature-based LAKM to build a secure network. A constructed secure network consists of authenticated vehicles for communication.
- ACR algorithm is implemented in the proposed model and its modified pheromone patterns are configured to handle a high concentration of pheromones in optimal paths to find efficient secure shortest paths for seamless data transmission.
- Novel optimal route discovery mechanism and route-handling mechanism of the proposed ACR are used to provide efficient routing and route handling for VANETs.
- Using an efficient and secure shortest path with secure seamless data transmission increases efficiency in routing in terms of high throughput, high packet delivery, low overhead, and low end-to-end delay.
- Furthermore, this work provides a comparison of ELAACR with existing schemes, i.e. EHACORP and F-ANT.

The rest of the manuscript is structured as follows. Section 2 is devoted to related work. The proposed work is described in Sect. 3. Section 4 covers simulation results and performance analysis and the last section concludes the proposed work.

2 Related Work

In the proposed work, a bio-inspired algorithm like an ant colony optimization (ACO) is combined with a group signature-oriented location-aided key management scheme to provide secure and reliable communication. In this context, this section provides a discussion of existing location-aided, group signature-oriented schemes and secure ACO-based works.

Muniyandi et al. [10] discussed the importance of location-aided routing (LAR) for dynamic VANETs. The authors found that LAR uses location information obtained from Global Positioning System GPS) sensors to locate nodes in the network. Using location information reduces the search space for a particular route, reducing the use of route discovery and route maintenance messages by limiting the search space to the communication range. It also helps to reduce the overhead. An extension for LAR [11, 12] improves the stability of routes by removing nodes based on direction. Nodes in the opposite direction to the origin are removed. The forward direction of nodes is considered based on the source direction for routing.

The work proposed by Gurumoorthi and Ayyasamy [13] is a combination of position-oriented and geocasting. The distance between vehicles is determined based on the current position of the vehicles. This work was carried out in two phases. In step 1, the source's next hop vehicles are selected for forwarding packets in the expected zone. In step 2, the geocast routing procedure is used and the desired zone is converted into a geocast region. This work proves the efficiency of position-oriented routing in terms of retransmission ratio and hop count. Pandey et al. [14] considered hop count as an important metric to evaluate the performance of VANET protocols. Enhanced Direction-Based Location-Aided Routing (DLAR) considers hop count and direction of vehicles for message forwarding. Route efficiency is estimated by hop count and duration. DLAR constructs routes with low overhead, minimum hops, and long lifetime.

Ali et al. [15] improve location-based routing by adding location privacy to vehicles. In this task, RSU helps vehicles with secure message transmission. A location privacy mechanism protects the vehicle's information from intruders. Message forwarding between source and target is achieved with highly efficient encryption/decryption techniques. This task provides location privacy protection for the entire routing process including vehicles, RSU, and intermediate cars. Additionally, end-to-end secure message forwarding is also a primary objective of this work.

The GPSR [16] (Greedy Perimeter Stateless Routing) is a most outstanding location-based routing convention. In GPSR stateless routing provides efficient paths. The greedy approach chooses legitimate nodes according to the greedy perimeter. Direction-Based Forwarding (DBF) [17] is a location-based steering convention that was originally presented by utilizing a predefined map direction (way) to control steering choices and forward bundles in a predefined way. The source indicates the direction of a parcel and forwards the packets in the specified direction toward the destination.

An authentication mechanism [18] based on a group signature scheme is proposed to authenticate vehicles as legitimate members of a group. Vehicle privacy is the main purpose of this work. This work focuses on V2V and V2R to provide secure communication by satisfying message integrity. Funderburg et al. [19] propose an improved group signature scheme to reduce pairing costs earned during pairing operations. Also, the cost of updating group key information is considered. The group signature has been modified to eliminate pairing operations and twin loads in key distribution systems. Pairing with the same private keys is eliminated to reduce the cost of the pairing operation. In Lu et al. [20] group signature allows any vehicle of the group to sign a packet anonymously on behalf of the group to provide privacy. This work proposes important changes to the group signature. Factors such as weight, reward, and punishment mechanisms are proposed to quantify the trustworthiness of shared information through a group signature scheme. Shangle Li et al. [21] use a double-key approach to satisfy the exculpability issue in group signatures. To address exculpability Shangle Li proposes a privacy-preserving scheme with group signature. This work combines group signature with an identity-based approach for offering trusted communication among vehicles, RSU, and trusted authorities.

Group signature [22] is used in VANETs to provide message authentication. Non-repudiation and unlinkability features combined to provide authentication functionality for vehicles and messages. Additionally, this work focuses on providing less burden by taking privacy and identity levels as a single scheme. Cryptographic and communication delays are analyzed to prove the efficiency of the routing scheme. This work also proves that transmitting messages with lower frequency provides quick delivery of urgent messages. A group signature [23] scheme allows vehicles to dynamically join a network to provide privacy for vehicle information. When joining a group, the group administrator authenticates the car and a group member certificate is generated for signing. The certificate is canceled when the vehicles leave the group. The proposed group signature scheme adds little overhead to improve the efficiency of the signature process. A group signature scheme with low overhead is suitable for dynamic networks.

To provide security [24] for messages transmitted between vehicles, a Certificate less aggregate signature (CAS) is proposed. This work applies CAS to a routing mechanism to provide vehicles with the ability to avoid leaking sensitive data during message transmission. CAS is suitable for implementation in VANETs to protect sensitive data. According to Lim et al. [25] a group signature mechanism is an ideal approach to protect message communication in VANETs from malicious users. The authors propose an effective key management approach based on a group signature scheme. A group is transformed into a domain with RSUs and vehicles to frame the topology. This mechanism securely exchanges group keys between vehicles. The use of Bloom filters improves privacy and security.

The work proposed by Chhikara and Patel [26] demonstrates ACO's robustness against failures and security. Artificial ants in ACO configure route information for routing. Only the information of the authenticated node is stored in the ant header for traveling between the source and destination. Saleem and Ahmed [27] use Enhanced Ant Colony Optimization (eACO) for secure routing of packets. eACO transmits packets securely by considering the header information of the packets. Encryption of header information in packets helps to protect packets from malicious nodes. eACO performs routing by considering the energy of nodes. The performance of eACO is evaluated in terms of PDR, overhead, and energy consumption. Zhang et al. [28] introduce security-aware fuzzy enhanced ACO for secure routing. The adoption of fuzzy logic with ACO improves the convergence speed of ACO. This task specifically identifies misbehaving nodes and avoids misbehaving nodes during routing. A fuzzy-oriented detection scheme robustly weights nodes based on limited information. This work also has the potential to provide a high level of robustness against blackhole and Sybil attacks.

Real-time message propagation in VANETs requires an energy-efficient shortest path without congestion to quickly deliver messages without delay. Ramamoorthy and Thangavelu [29] proposed an efficient routing scheme based on congestion and residual energy of nodes. Distance, congestion, and energy levels of nodes are key factors for route formation. This work focuses only on finding efficient routes but fails to provide security for paths. This work uses ACO with modified pheromone models for path establishment, data transfer, and path maintenance.

Maranur and Mathapati [30] introduce an ACO-based routing scheme for routing in VANETs. ACO uses a trust-based fitness function to compute a trust value for each node. Important reliability parameters used in trust value calculation are link quality, mobility, and buffer capacity. Routes are identified based on trusted values. Patel and Jhaveri [31] use ACO to send data packets to targets based on nodes' trust values. Security mechanisms are used to establish secure paths between the source and destination. Paths are safe from malicious attacks. ACO combines with a group signature scheme to establish routes. Source, destination, and intermediate nodes are authenticated before starting data transmission.

Anantapur and Patil [32] proposed an ACO-based modified ad hoc on-demand distance vector (MAODV) to provide secure packet transmission over ad hoc networks. ACO in MAODV calculates fitness functions based on belief, distance, node degree, and residual energy. A fitness value gives the fitness of a path, and the safest path is rich in fitness value. The route discovery method finds optimal routes based on fitness values. Essentially it improves AODV performance and prevents blackhole attacks to provide better packet transmission.

In Maheshwari and Bhardwaj [33] for secure route selection, the route selection parameter (RSP) is calculated at each node. RSP at each node is calculated based on packet forwarding ratio, cost, and bandwidth capacity. The route discovery mechanism selects intermediate nodes for routes with high RSP values. A path with a good packet forwarding ratio provides maximum delivery of packets and the authors consider this path to be more secure. Choosing a path with a higher capacity of bandwidth ensures faster delivery of packets.

A modified ACO [34] is used to establish the efficient shortest path based on the distance metric. Efficient routing is suitable for high packet delivery and throughput. A modification to ACO improves its convergence speed for low-density networks. When the network size increases dynamically, the convergence speed of ACO decreases. In the Enhanced Bio-Inspired Routing Algorithm (EBIRA) [35], Enhanced ACO finds routes based on distance, hop count, and signal strength. Routes identified in EBIRA are more efficient for routing with less overhead. Enhanced ACO generates less overhead for massive network changes, in turn increasing network performance.

Ramamoorthy and Thangavelu [36] proposed an EHACORP to improve the efficiency of the routing process with the shortest paths. EHACORP combines ACO with source-based routing for efficient route discovery. Multiple paths are identified and the most efficient path among the multiple paths is identified. The source specifically implements a route selection algorithm to select efficient routes. The efficiency of routes is determined based on hop count and distance. The source initiates route handling packets to repair the route for link breaks. EHACORP proves its efficiency in different road scenarios with different vehicle variations.

Fatemidokht and Kuchaki Rafsanjani [37] introduced F-ANT for efficient routing in VANETs. F-ANT uses ACO and fuzzy logic to estimate efficient routes, efficient routes are rich in providing optimal message dissemination. The efficiency of a path is determined based on the connectivity level of the links and the capability levels of the nodes. Connectivity levels deal with signal strength and the level of congestion of links. Capacity levels of nodes deal with bandwidth. ACO initiates the route discovery process to find routes based on connectivity and capability levels. NS2 was used to simulate F-ANT. Simulation results were conducted for real-time traffic scenarios and F-ANT outperformed in all aspects compared to on-demand and proactive protocols.

The position-based ACO [38] relies on the exact GPS-based location of vehicles and mobility directions to find stable paths. The location servers play a vital role in exchanging location information of vehicles. Routing tables are updated proactively to have up-to-date routing information. However global positioning will not be suitable for roads with tunnels. The proactive-based ACO [39] will quickly find optimal paths for VANETs, but periodic updates are necessary to maintain stable paths. The overhead is very high because the frequent exchange of routing information is required. The reactive-based ACO [40] is very suitable for VANETs. The paths are determined based on demand but a significant delay can occur. Hybrid ACO [41] combines proactive and reactive together to offer message routing. The transmission range of each vehicle is very important for hybrid routing. The proactive method is used to transmit a message within the geographical area of each node. The reactive method is utilized for routing the packets between the networks.

Multipath ACO [42] is suitable for continuous data transmission applications. Many paths will be elected for routing and data will be distributed among paths to reach the targets. Unicast ACO-based [43] methods will unicast data with a single path. Unicast ACO-type algorithms are not suitable for VANETs. The Quality of service (QoS) [43] based ACO algorithms have to satisfy many QoS metrics in routing. High-quality paths in terms of connectivity, robustness, adaptability, and efficiency are used in QoS routing. QoS-based routing will produce high overhead in routing. However significant benefits are high throughput with low latency. Furthermore, many ACO-based algorithms have been announced in the last decade to provide efficient routing. Certain modifications happen in traditional ACOs to improve their working style for increase its convergence speed. Table 1 summarizes existing position-based, group signature-oriented location-aided key management schemes and ACOs. This table presents scenarios, evaluation parameters, and tools/simulations of existing works.

In Table 1, Packet Delivery Ratio (PDR), End to End delay (E2E), Routing Overhead (RO), Throughput (T), Packet loss rate (PLR), Normalized routing load (NRL), Vehicle to RSU (V2R), Packet lost rate (PLR), Network Simulator (NS2), Certificate less aggregate signature (CAS).

3 Proposed VANET System

In this work, ELAACR is proposed to achieve seamless secure data transmission. The proposed VANET system works in two phases. Phase 1 implements a location-aided key management (LAKM) scheme based on group signature (GS) to establish a secure network, and Phase 2 uses ACR to find efficient secure paths for seamless data transmission. In Phase 1, the GS is computed among the vehicles in the network. The pair of public and private keys used for GS. GS allows any vehicle on the network to become a legitimate member of the group by signing the GS using the group's public key and the vehicle's private key. Wireless medium-based communication is more vulnerable to security issues but using a group signature scheme allows the proposed system to build a secure network.

In Phase 2, ACR is triggered to find an efficient secure path for seamless data transmission based on the pheromone concentration of the path. ACR uses Route Explorer Ants (REANTs) and Route Manage Ants (RMANTs) to discover routes. During new route discovery, REANTs deposit pheromones on the routes, and RMANTs update the pheromone-based on the old pheromone value and evaporation rate. RMANTs also calculate the pheromone summation for each route. A path with a higher pheromone value and lower hop

Table 1 Summarization of existing works

References	Scenarios	Parameters used for evaluation	Tool/simulator
Muniyandi et al. [10]	V2V and V2I	PDR, E2E, RO, Energy consumption	MATLAB
Reka et al. [11] and Raghu et al. [12]	V2V and V2I	E2E, Path Stability, PDR, NRL, and T	NS2
Gurumoorthi and Ayyasamy [13]	V2V and V2I	PDR, E2E, Hop count, and retransmission ratio	NS2
Pandey et al. [14]	V2R and V2V	Path duration and Hop count	MATLAB
Ali et al. [15]	V2V and V2I	Transmission delay, PDR	NS2
Karp and Kung [16]	V2V and V2I	Path length, PDR, and RO	NS2
Aluvala and Rajasekhar [17]	V2V and V2I	PDR and RO	NS2
Sudarsono [18]	V2R and V2V	Processing time and Revoke check time	–
Funderburg et al. [19]	V2V and V2I	Authentication, Privacy, and Efficiency	NS2
Lu et al. [20]	V2V and V2I	Signature Verification time	NS2
Shangle Li et al. [21]	V2R and V2V	Computation cost, Time needed for signature and verification	Cryptographic library
Zhang et al. [22]	V2V and V2I	Total average delay and Cryptographic delay	NS2
Liu et al. [23]	V2I	Computational overhead	NS2
Cahyadi et al. [24]	V2R and V2V	Computation and communication overheads	NS2
Lim et al. [25]	V2I	Key establishment, Utilization, and Communication Overhead	NS2
Chhikara and Patel [26]	V2I	ACO API with the network vulnerability tool	Java/Webserver
Salim and Ahmed [27]	MANET topology	PDR, RO, Energy consumption	NS2
Zhang et al. [28]	MANET topology	PDR, EED, and RO,	NS3
Ramamoorthy and Thangavelu [29]	V2V	PDR, E2E, RO, Energy consumption	NS2
Maranur and Mathapati [30]	V2V	T, EED, RO, Time and Space Complexity	NS2
Patel and Jhaveri [31]	V2V	PDR, E2E, RO, Energy consumption	NS2
Anantapur and Patil [32]	MANET topology	T, PDR, E2E, and RO	NS2
Maheshwari and Bhardwaj [33]	MANET topology	Congestion level of links	Mathematical Models
Ramamoorthy and Thangavelu [34]	V2V	PDR, RO, EED, Communication cost	NS2
Ramamoorthy and Thangavelu [35]	V2V	PDR, Latency, and T	NS2
Ramamoorthy and Thangavelu [36]	V2V	PDR, E2E, RO, PLR, and T	NS2
Fatemidokht and Kuchaki Rafsanjani [37]	V2V	PDR, E2E, RO, PLR, and T	NS2

count is selected for data transmission. Notably, during the route discovery phase, ACR uses the GS scheme to bring all vehicles of identified routes under a legitimate group. A legitimate group is a group consisting of vehicles that have been authenticated using the GS scheme. After selecting a path based on the pheromone summation value and hop count Data Carry Ants (DCAs) are created to transmit data between the source and destination using a secure established path. To handle link failures, ACR includes a route-handling mechanism. This mechanism maintains and repairs link breaks. Route Error Handling Ant (REHANT) and Acknowledgment ANT (AKANT) are used in the route handling mechanism.

Figure 2 illustrates the phases of ELAACR. In ELAACR, vehicles are positioned randomly. The LAKM (Phase 1) approach computes GS. The ACR (Phase 2) is combined with LAKM to find an optimal and efficient secure path for seamless data transmission. ACR has an optimal route discovery mechanism for optimal route selection. The optimal route selection procedure enables REANTs and RMANTs to find several suitable routes, and the best optimal route is selected among the identified routes based on pheromone summation and vehicle count. ACR uses a route handling mechanism to efficiently handle sudden link breaks. In ELAACR, the network (N) includes a group of moving vehicles. N consists vehicles $\left(V1, V2, \ldots, V_n\right)$ and links $\left(L1, L2, \ldots, L_n\right)$. The links associate vehicles in N.

3.1 Phase 1: Location-Aided Key Management (LAKM) Scheme

LAKM relies on the GS method to construct a secure network. The GS is a key signature scheme with privacy features. In GS any legitimate member (vehicle) of the network can sign a forward packet using its private key and group public key. A GS is created with private and public keys. Any vehicle in the network can decrypt the signed packet by using a key pair such as public and private keys.

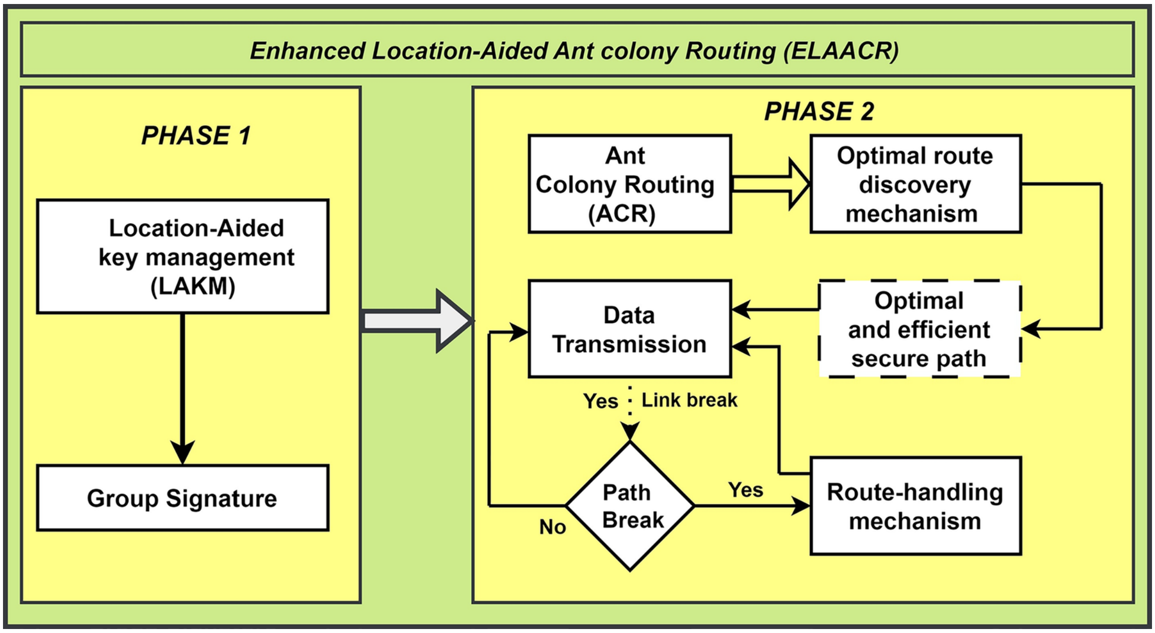

Enhanced Location-Aided Ant colony Routing (ELAACR)
PHASE 1
Location-Aided key management (LAKM)
Group Signature
PHASE 2
Ant Colony Routing (ACR)
Optimal route discovery mechanism
Data Transmission
Optimal and efficient secure path
Yes
Link break
Path Break
Yes
No
Route-handling mechanism

Fig. 2 Architecture of ELAACR

A valid GS implies that the vehicle is a bonafide member of the group. Conversely, assuming two valid group signatures, determining whether they were produced by similar (or different) group members is computationally impossible. If a disagreement arises on a group signature, a distinct entity such as Group Manager can ask to open the signature and identify the genuine signer. This activity is denoted as Escrowed Anonymity. Based on anonymity, the GS is suitable for VANETs to impose security. The Vehicle can sign GS with its current location without tracking. The LAKM uses an offline group Manager (OGM) to initiate the GS scheme and enroll all vehicles as members in a group.

3.1.1 Phase 1 Needs the Following Specific Requirements to Construct a Secure Network

- LOCATION: All vehicles in VANET must obtain their exact location reliably and securely using a GPS.
- TIME: Vehicles in VANET should keep loosely synchronized clocks. These clocks can be obtained from the GPS.
- RANGE: Uniform transmission range allotted to all vehicles as per Dedicated short-range communication (DSRC) and IEEE 802.11p. This allotment helps to find one-hop nodes for each vehicle.
- MOBILITY: All nodes move randomly in the network according to the mobility model for a fixed amount of time.

3.1.2 Entities of GS

- *Group Manager (GM)*: Accountable for grouping the vehicles. GM allows vehicles to join and leave. De-anonymizing the signature for dispute is also the duty of GM. GM distributes the public key to all its members.
- *Legitimate Group Member (LGM)*: Authorized vehicles in the group. LGMs consist of private keys. This private key is used by the vehicle to sign the GS on behalf of a group.
- *Outside Vehicles*: Vehicles that do not belong to the group. All these vehicles are eligible to become group members at any time.

3.1.3 Components of GS

- *SETUP*: A polynomial time series method to output cryptographic keys such as public and private keys. The setup component is initially run by GM.
- *JOIN*: A secure protocol between a new vehicle (wish to join a group) and GM. The output of this component is the private key for group members.
- *SIGN*: A procedure run by a group member to generate GS using public and private keys.
- *VERIFY*: Any member can verify GS using its private and group public key.
- *OPEN*: Run by GM when a dispute occurs on GS.
- *REVOKE*: Run by GM to withdraw the public key and dissolve the membership of the entity from the group.

3.1.4 Operations of LAKM

Step 1: Each vehicle broadcasts a hello packet with its information such as location, group public key, and time stamp. The GS is computed by using the above information. Each vehicle broadcasts its hello packet to its one-hop neighbors.

Step 2: While receiving a hello packet, each vehicle verifies GS by using its private key and group public key. If verification is successful, the vehicle re-broadcasts the hello packet to its one-hop neighbors for the next verification. Equation 1 indicates the elements of the hello packet. Figure 3 demonstrates how hello packets are broadcasted to the neighbors of each vehicle.

$$\begin{aligned} Temp_{id} &= \big(\big(Location_{GPS\ Coordinates} \,||\, Group\ Signature_{\ Public,private\ keys}\big) \\ &\qquad Temp_{Key} = Key_{Number}\big) \end{aligned} \tag{1}$$

In Eq. 1, $Temp_{id}$ is a temporary identity allotted for the hello packet. $Location_{\ GPS\ Coordinators}$ are the X and Y coordinates of vehicles. *Group signature* is the signature computed between vehicles. $Temp_{Key}$ is the temporary key used in the GS scheme.

3.2 Ant Colony Routing (ACR)

ACR is the foremost practice for finding the best routes using pheromones. ACR uses the analogy of ACO to find the optimal paths as shown in Fig. 3. The analogy and behavior of ACO is a natural behavior. The ACO consists of artificial packets called ants such as $\mathrm{FWD}_{\mathrm{ant}}$ and $\mathrm{BWD}_{\mathrm{ant}}$ to find the road to food sources. When no path to a food source, the $\mathrm{FWD}_{\mathrm{ant}}$ travels towards the destination by depositing the chemical substance called pheromone on their traveled path. All successful $\mathrm{FWD}_{\mathrm{ant}}$ are converted into $\mathrm{BWD}_{\mathrm{ant}}$ in the destination. $\mathrm{BWD}_{\mathrm{ant}}$ travels in the reverse direction of $\mathrm{FWD}_{\mathrm{ant}}$ to reach the source. At the same time, the $\mathrm{BWD}_{\mathrm{ant}}$ updates the pheromone on its path. This analogy is considered in the proposed work to find the optimal routes. Table 2 shows the algorithm of ACR. As per the algorithm, the ACR initializes all required parameters, pheromone models are called to deposit and update the pheromone on the path until facing the end criteria. Figure 4 represents the movement of ants such as how $\mathrm{FWD}_{\mathrm{ant}}$ and $\mathrm{BWD}_{\mathrm{ant}}$ travel between the origin and target to find valid routes. The $\mathrm{FWD}_{\mathrm{ant}}$ ants move towards a destination in the forward direction until they reach the destination. The successful $\mathrm{FWD}_{\mathrm{ant}}$ transformed into $\mathrm{BWD}_{\mathrm{ant}}$ to bring route information to the source.

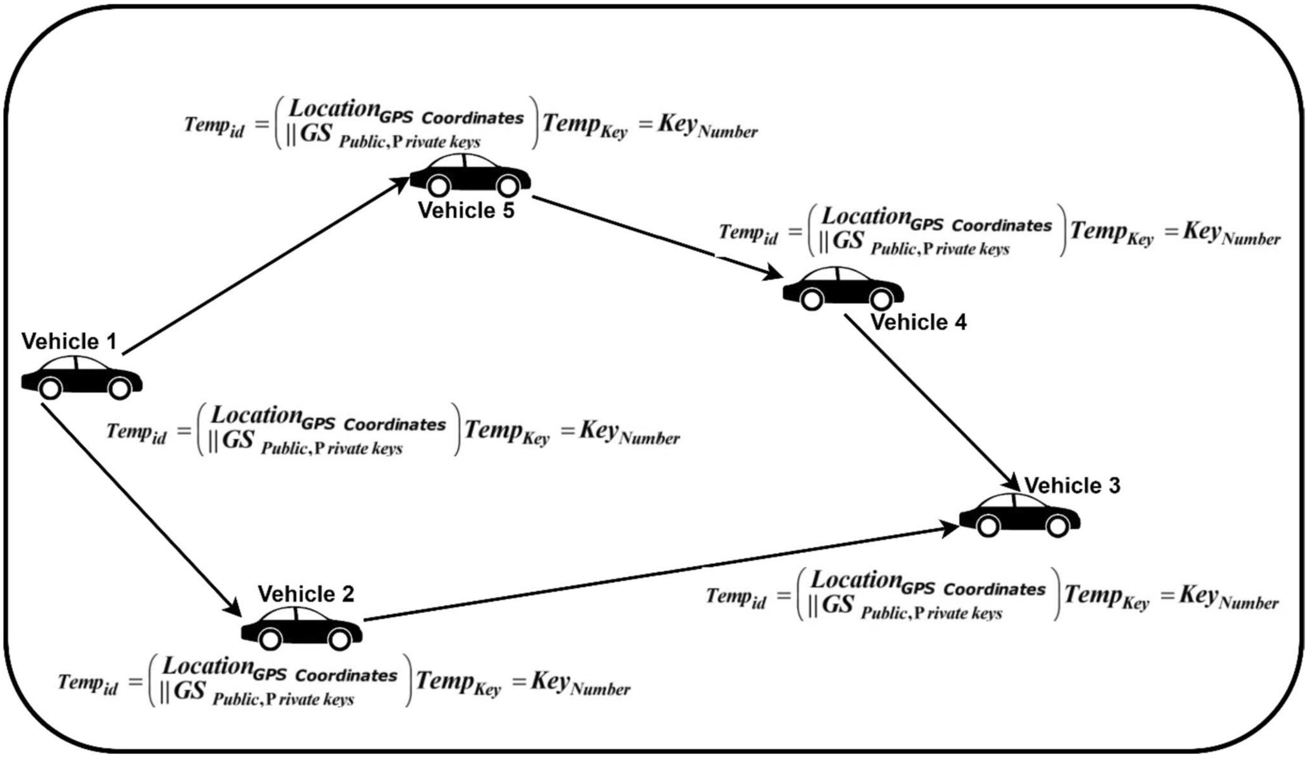

Temp_id = (Location_GPS Coordinates || GS Public,Private keys) Temp_Key = Key_Number
Vehicle 5
Temp_id = (Location_GPS Coordinates || GS Public,Private keys) Temp_Key = Key_Number
Vehicle 4
Vehicle 1
Temp_id = (Location_GPS Coordinates || GS Public,Private keys) Temp_Key = Key_Number
Vehicle 3
Vehicle 2
Temp_id = (Location_GPS Coordinates || GS Public,Private keys) Temp_Key = Key_Number
Temp_id = (Location_GPS Coordinates || GS Public,Private keys) Temp_Key = Key_Number

Fig. 3 Hello packets broadcasting

Table 2 ACR-algorithm

```
ACR-algorithm

Describe factors
Initiate Pheromone trails
While (end conditions not encountered) do
Build schedules
    Call local
    Initiate hunt
    Update pheromone on route
    Find paths
End of run
```

3.2.1 Phase 2 Needs the Following Specific Requirements to Establish a Secure and Efficient Path

The ACR should be configured as follows to find routes.

- The ACR should be configured dynamically to adjust pheromones based on control coefficients.
- ACR has to generate REANT to find a route with the coordination of Phase 1.
- ACR has to generate RMANT to manage the path and to bring path information to the generator of REANT.
- ACR must have the ability to create REHANT to handle broken routes.
- ACR has to create a DCA for sending data from source to destination.

3.2.2 Optimal Route Discovery Mechanism

When a source does not have a usable route to a destination to send data packets, a valid route must be determined by a routing mechanism. The ACR is utilized to discover the secure shortest path to a destination. To discover a valid route, the ACR requests REANT. The REANTs are created in source based on their neighbor table. Each vehicle maintains a neighbor table to keep the tract of one-hop nodes based on mobility. The REANTs start their journey toward the destination by following phases 1 and 2. REANTs pass from vehicle to vehicle toward the destination by following the probability rule and pheromone deposit formula. The structure of REANT is shown in Eq. 2. Equation 3 shows the probability rule and Eq. 4 represents the pheromone deposit formula. Equation 5 depicts the measurement of pheromones. Equation 6 shows how HOP_{count} is computed.

$$REANT\left(S_{No}, S_{add}, D_{add}, HOP_{count}Add_{\,\text{Record}}, GS_{\,public,private\ Keys}, \Gamma_{i,j}\right) \tag{2}$$

In REANT, S_{No} is the sequence number used to discard duplicates, S_{add} is the source address, D_{add} is the destination address, HOP_{count} is the vehicle count. It indicates the total number of vehicles visited by REANT during its journey toward its destination. $Add_{\,\text{Record}}$ is the record of vehicles, and the travel history contains identities of visited vehicles by REANT. $GS_{\,public,private\ Keys}$ indicates group signature computed between two vehicles. $\Gamma_{i,j}$ is the pheromone deposited by REANT.

$$p_{o,p} = \frac{\Gamma^{\alpha}_{o,p}\eta^{\beta}_{o,p}}{\sum \Gamma^{\alpha}_{o,p}\eta^{\beta}_{o,p}} \tag{3}$$

Equation 3, $\Gamma^{\alpha}_{o,p}$ is the measure of pheromone on anxiety o, p. α is a metric to regulate the effect of $\Gamma_{o,p}$. $\eta_{o,p}$ is the attractiveness of edge o, p. β is a metric to regulate the effect of $\eta_{o,p}$.

The volume of pheromone is deposited on the link between o, p using Eq. 4. The REANT deposits the pheromone on the path.

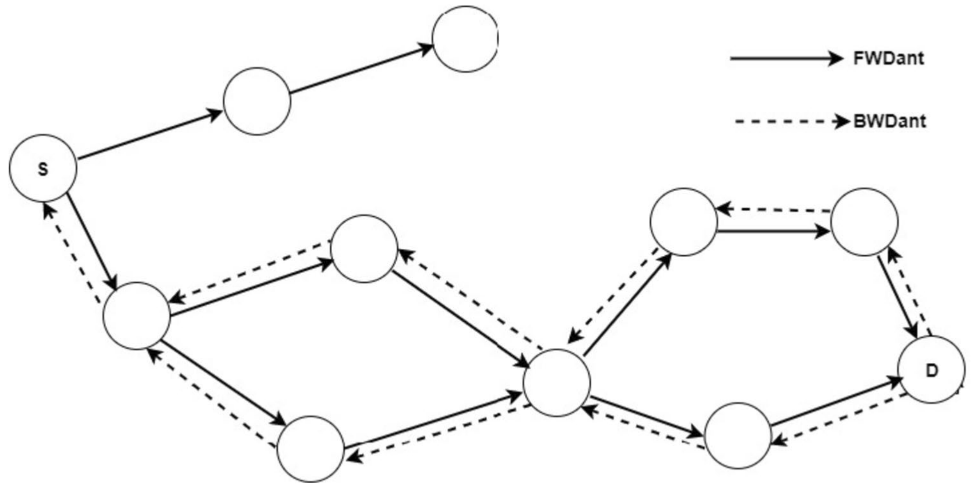


Fig. 4 Movements of ants toward the destination in ACR

$$\Gamma_{o,p} = \Gamma_{o,p} + \Delta\Gamma_{o,p} \tag{4}$$

where $\Gamma_{o,p}$ is the total volume of pheromones deposited by REANT. $\Delta\Gamma_{o,p}$ s the measure of pheromones that need to be deposited based on Eq. 5.

$$\Delta\Gamma_{o,p} = \begin{cases} \frac{1}{Lh_z} & if\ ant\ z\ moves\ on\ link\ o,p \\ 0 & otherwise \end{cases} \tag{5}$$

where Lh_z is the cost of the zth ant's visit.

$$HOP_{COUNT} = HOP_{COUNT} + 1 \tag{6}$$

Initially, HOP_{COUNT} value is set to zero, and for every visit, its value is incremented by 1. Pheromone quantity is refreshed by the RMANT ants. All successful REANTs at a destination are converted into RMANTs and refresh the pheromone on the return path based on Eq. 7. The Add_{Record} of REANTs copied to Add_{Record} of RMANTs.

$$\Gamma ph_{i,j} = (1-\rho)\Gamma_{i,j} + \sum_{k=1}^{m} \Delta\Gamma_{i,j} \tag{7}$$

In Eq. 7, ρ is the pheromone rate evaporation, $\Gamma_{i,j}$ is the old pheromone value, $\Gamma ph_{i,j}$ is the pheromone refreshed by RMANT towards the destination to source. All RMANT reach the source by refreshing the pheromone on their way to the source. Equation 8 Shows the structure of RMANT.

$$RMANT\left(S_{No},\ S_{add}, D_{add}, HOP_{count}Add_{\text{Record}},\ GS_{public,private\ Keys},\ \Gamma ph_{i,j}, Ph_{SUM}\right) \tag{8}$$

Fields of RMANT is similar to REANT except $\Gamma ph_{i,j}$ and Ph_{SUM}. $\Gamma ph_{i,j}$ is the pheromone refreshed by RMANT. The Ph_{SUM} is the consolidation of pheromones from destination to source. The Ph_{SUM} is computed via Eq. 9.

$$Ph_{SUM} = \sum \left(\Gamma ph_{i,j}.D_{Add}^{Add_{\text{Record}}}\ :\ \Gamma ph_{i,j}.S_{Add}^{Add_{\text{Record}}} \right) \tag{9}$$

Equation 9, Ph_{SUM} is the summation of pheromones from destination to source. Once RMANTs reach the source from the destination, the RMANT with a high pheromone and low hop count is selected for path construction. The Add_{Record} of RMANT is copied to the header of Data Carry Ant (DCA). Equation 10 shows the format of DCA. Table 3 displays the route selection algorithm executed at the source after receiving RMANT. The source executes a route selection algorithm to select an optimal route for routing the packets. This algorithm outputs optimal paths based on pheromone summation and hop count, which are extracted from RMANTs.

$$DCA(S_{No},\ S_{add}, D_{add}, Add_{\text{Record}}, Payload) \tag{10}$$

In Eq. 10 payload indicates the content of DCA.

Table 3 Route selection algorithm

```
Algorithm: Route selection algorithm
In Source (S):
S → After receiving RMANTs {
Select → RMANT = max (($Ph_{SUM}$) and min ($HOP_{count}$));
Read → Selected RMANT and Allot ID for selected Route;
Copy $Add_{\text{Record}}$ of RMANT and Route ID to DCAs;
Send data (S, D) through DCAs;
}
```

3.2.3 Route-Handling Mechanism

The communication links in the path are more vulnerable due to mobility. After a certain time, the vehicles can move from the established path, which ends with path breaks. To handle link breaks efficient route-handling mechanisms are necessary. This work considers that the source receives acknowledgment ants (AKANTs) for all transmitted packets. The source fails to receive AKANTs only when packets do not reach the target. The segmentation and re-segmentation are followed based on window size. This work considers equal window sizes at the source and destination. When the source fails to receive acknowledgments, it assumes a path break happens and stops sending DCA ants. If the link fails, the vehicle adjacent to the failed link initiates a REHANT. REHANT is transmitted downstream to the source vehicle on the current route to warn of link failure. When the source vehicle receives REHANT, Add_{Record} of DCA is immediately cleared. Similarly, the source ignores previously used routes for data transmission based on the route ID. Next, the source vehicle calls the route handling process to select another efficient route for data transfer. Once the route is identified after the link break, the Add_{Record} of RMANT is copied to DCAs Add_{Record}, and route ID is allotted to start data transmission. Equation 11 indicates REHANT and Eq. 12 indicates AKANT. Table 4 represents the algorithm for the route handling process.

$$REHANT\left(S_{No},\ S_{add}, D_{add}, Add_{\text{Record}}\right) \tag{11}$$

$$AKANT\left(S_{No},\ S_{add}, D_{add}, Add_{\text{Record}}\right) \tag{12}$$

Consider Fig. 5 and accept that the link between vehicle M and vehicle O is broken. In ELAACR, the source commonly gets AKANT from the destination for successful packets. A link failure arises when a destination vehicle or an intermediate vehicle deviates from the predetermined path. When the source is unsuccessful in receiving AKANTs from the destination, the source interprets this as a link failure because the packets can not practice delay or loss if an efficient shortest path is used. The vehicle adjacent to the

Table 4 Route handling process

```
Algorithm: Route handling process

In Source (S):
S → After receiving REHANT {
S → clears $Add_{Record}$ of DCAs;
S → Discards previously used route;
Route → Select. RMANT = max ($(Ph_{SUM})$ and min $(HOP_{count})$);
Read → Selected RMANT and Allot ID for selected Route;
Copy $Add_{Record}$ of RMANT and Route ID to DCAs;
Send data (S, D) through DCAs;
}
```

failed link (vehicle M) initiates REHANT and transmits it to the source. When receiving a REHANT, the source discards the route and calls the route handling process.

4 Simulation Results

4.1 Environment for Simulation

The proposed ELAACR and existing works EHACORP [36], and F-ANT [37] are implemented in NS 2.35 using C++ and Object Tool Command Language (OTcl). NS 2.35 is an open-source event-oriented simulator that is frequently employed in communication networks to simulate routing systems. To construct road scenarios for VANETs, the Java-based Mobility model generator for vehicular networks (MOVE) is utilized. MOVE is assembled on top of SUMO 0.22.0 (simulation of urban mobility). SUMO 0.22.0 is an open-source simulation platform utilized to simulate traffic in the VANET environment. SUMO 0.22.0 enables simulation of VANETs environment for ELAACR in integration with OpenStreetMap and MOVE. For simulation, the Hosur to Bengaluru highway (Part of the national highway) from OpenStreetMap is exported in the type of Extensible Markup Language (XML) such as osm.xml type and used this exported map as the road map for simulation. The exported XML file is converted into net.xml using net convert. The traffic modeler imports net.xml to produce traffic scenarios. The traffic modeler is a graphical user interface utilized to create vehicular traffic. TraNSLite is used for converting created traffic scenarios into Tool command language (TCL) for execution in NS 2.35. Figure 6 shows the simulation steps used in the implementation of the proposed work and existing works.

The metrics such as T, PLR, PDR, OH, and EED, and according to the simulation period the average of EED and PDR is used to evaluate the performance of the proposed and existing works. Vehicle variations from 30 to 200 were used in the simulation to examine the results of the ELAACR, EHACORP, and F-ANT. In the simulation, IEEE 802.11p

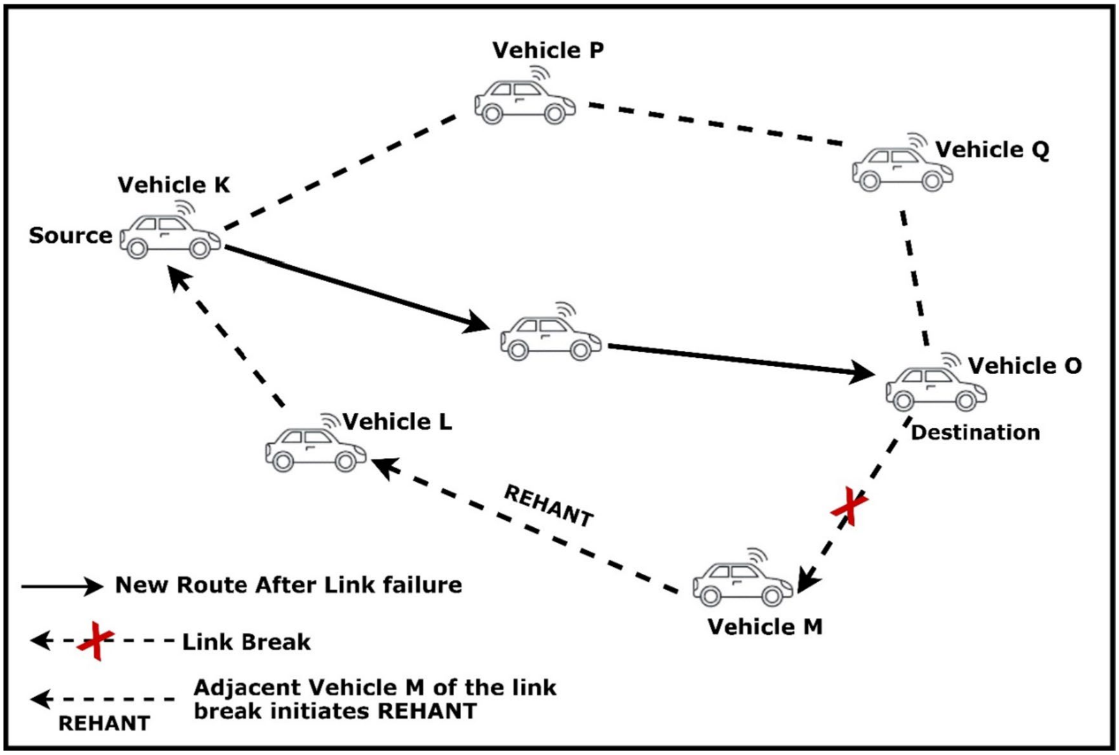


Fig. 5 Route handling scenario

is utilized. It can provide a vehicle speed of 30 m/s (around 110 km/h) for urban, rural, and suburban environments. Dedicated short-range communication (DSRC) is used to consider the transmission range of each vehicle up to 350 m. The constant bit rate (CBR) model is followed to produce the traffic at a constant rate. The ACR algorithm in the proposed work follows the evaporation rate of 0.2, 0.3, 0.6, and 0.8. The tests were kept running for the accompanying packet sizes 512, and 1024 bytes. The performance of ELAACR, EHACORP, and F-ANT were analyzed for metrics with different vehicle variations and packet sizes. Table 5 gives the complete parameters set used in the simulation.

4.2 Why are the Proposed ELAACR and the Existing EHACORP and F-ANT Tested in a Real-Time Road Scenario?

VANET is subject to normal changes in terms of vehicle variations. Road density is not the same in all cases. The validity of vehicles can change at any time to raise frequent network changes. To follow real-time road conditions for proposed and existing works, the Hosur to Bangalore highway from OpenStreetMap is considered. This observation helps to test all approaches by considering real-time traffic. Figure 7 shows the OpenStreetMap of Hosur to Bangalore highway imported from OpenStreetMap. Figure 8 shows the real-world mode of Sumo-gui bengaluru.sumo.cfg, used in the simulation. Different vehicle variations such as 30, 40, 50, 100, 150, and 200 are considered as scenarios or case studies to evaluate the behavior of the proposed and existing protocols in real time. Vehicles follow a speed of 0 to 30 m/s (about 110 km/h). Simulation tests follow different packet sizes such as 512 and 1024 bytes. Different variations such as packet sizes and vehicles helped to practically prove the efficiency of the proposed and existing works.

Table 5 Parameters set

Parameters	Value
Simulation period	500 s
MAC type protocol	IEEE 802.11p
Communication covered	350 m
Vehicle variations	20–200
Speed	0–30 m/s
Road map size	850×900
Propagation type model	Two-ray ground
Traffic model	CBR
Data packet size	512 bytes, and 1024 bytes
Mobility based model	SUMO
Simulator	NS 2.35

4.3 Impact and Limitations of the Proposed ELAACR in VANET Environments

VANETS supports both highway and urban environments. A highway environment consists of only a few barriers and traffic signals. Vehicles face high speeds and rely on multi-hop communication to exchange messages between vehicles. An urban environment consists of different entities such as intersections, streets, traffic signals, crosswalks, buildings, etc. The availability of these entities affects signal transmission, which ends in packet loss. Additionally, vehicle speeds vary irregularly in urban environments due to traffic lights, crosswalks, and barriers; Hence, vehicles experience high variations in speed in this environment. Mobility assessment in urban environments is difficult. This study focuses on the implementation of the proposed ELAACR and existing works in a highway environment (Hosur to Bengaluru Highway: Part of the National Highway). ELAACR is compatible with the highway environment in the following ways.

Scalability: The ACR of ELAACR has the scalability to create REANT and other ants for different types of vehicles (30, 40, 50, 100, 150, and 200). ACR can generate many

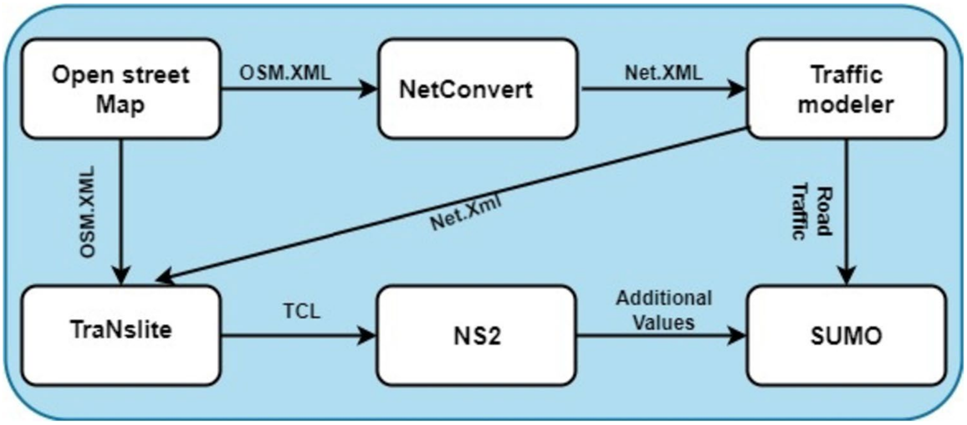


Fig. 6 Simulation steps

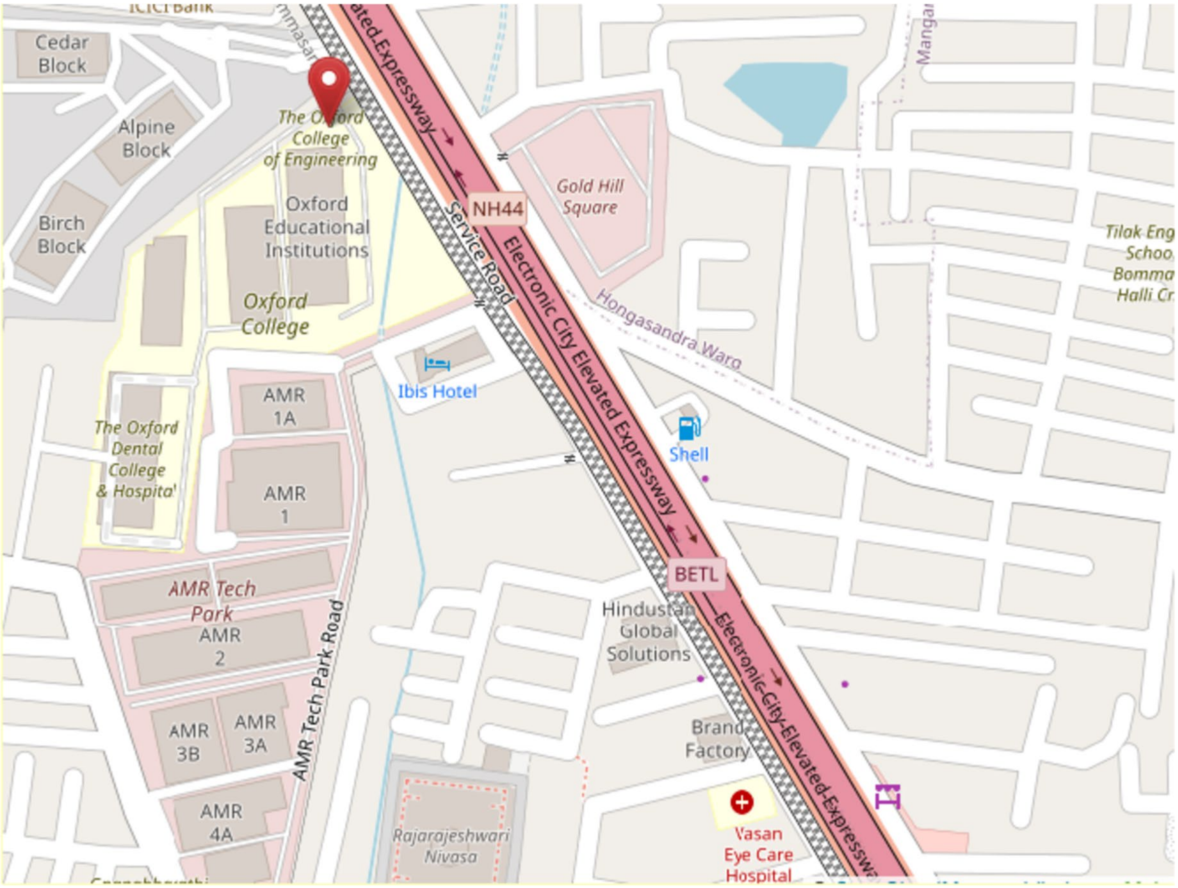


Fig. 7 OpenStreetMap for Hosur to Bengaluru highway

types of ants and adjust them according to network size and variations. Indirect communication between ants in ACR provides more scalable solutions for large-scale networks such as VANETs.

Adaptability: ELAACR's ACR is suitable for self-organized networks based on highly collaborative tasks. ACR's ants can perform assigned tasks based on a distributed method without human intervention. The behavior of ACR ants is deterministic. According to network changes, ants can be deployed for the ACR routing mechanism.

Fault tolerance: In ACR, link outage/interruption does not lead to catastrophic failures. ACR follows a strictly decentralized control system. Lack of specific vehicles or link breaks does not reduce routing performance.

Limitations of proposed ELAACR: The proposed ELAACR is implemented for highway road scenarios and finds optimal shortest paths for routing based on hop count and pheromone summation (intensity). However, in an urban environment, the high number of traffic signals and highly non-uniform speeds affect the density of vehicles on the road. In urban situations, ELAACR mechanisms can find the shortest routes with a large number of vehicles as hop count for routing, which increases the processing overhead. Further research is needed to refine ELAACR for urban environments.

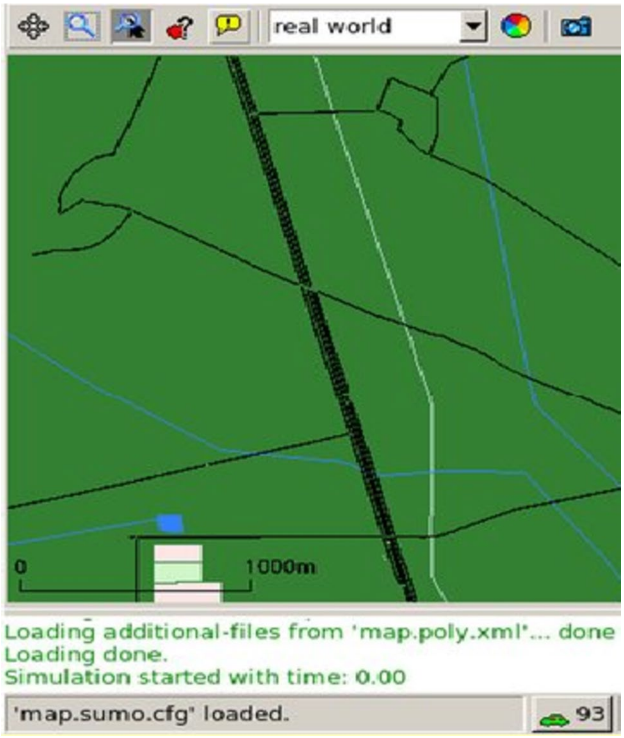
4.4 The Proposed ELAACR is Compared with EHACORP and F-ANT, Why These Protocols?

The proposed ELAACR uses ACR in the routing mechanism, similarly, EHACORP and F-ANT also rely on ACO for the routing mechanism. ACO in EHACORP and F-ANT determine the shortest path with minimum hops between origin and destination. The proposed ELAACR relies on ACR to find a secure path with minimum hops. The reliance of EHACORP and F-ANT on Ant colony oriented routing raises grounds for comparing them with the proposed ELAACR. Table 6 depicts the comparison of ELAACR with existing works.

4.5 Evaluation Metrics

The ELAACR, EHACORP, and F-ANT are evaluated for the following metrics.

Throughput (T): T indicates the amount of data transmitted for the amount of time T_t. T can be evaluated via Eq. 13.



Loading additional-files from 'map.poly.xml'... done
Loading done.
Simulation started with time: 0.00
'map.sumo.cfg' loaded.

Fig. 8 A scenario of the Hosur to Bengaluru highway in the SUMO tool

$$T = \left(\frac{\sum_{k=1}^{m} \text{Packets received}}{T_t} \right) \quad (13)$$

Packet loss rate (PLR): PLR is the value for packets received for transmitted packets. Equation 14 is used to calculate PLR.

$$PLR = \left(\sum_{l=1}^{m} \text{Packets sent} - \sum_{l=1}^{m} \text{Packets received} \right) \times 100 \quad (14)$$

Packet delivery ratio (PDR): PDR gives the total percentage of packets received to the whole packets sent. Equation 15 is used for calculating PDR.

$$PDR = \left(\frac{\sum_{m=1}^{l} \text{Packets Received}}{\sum_{\mathrm{i}=1}^{\mathrm{n}} \text{Packets Send}} \right) \quad (15)$$

Overhead (OH): OH is the percentage of whole data packets to total routing packets. Equation 16 is used to compute OH.

$$OH = \left(\frac{R_P}{D_P} \right) \quad (16)$$

End-to-End Delay (EED): EED is the time calculated from packet starting time to its reached time to destination. Equation 17 calculated EED.

$$\text{EED} = \sum (\text{Packet Reached Time - Packet Starting Time}) \quad (17)$$

4.6 Performance Analysis

In the performance analysis section, ELAACR performance is compared with EHACORP and F-ANT.

4.6.1 Throughput (T)

Using a seamless secure shortest route with a restricted number of intermediate vehicles improves the throughput of the proposed ELAACR. In the proposed ELAACR, the group signature is used for establishing a secure route and the modified ACR is used to establish efficient and reliable paths for routing. The EHACORP concentrates only on finding the shortest path but not a secure and seamless path. Using group signatures provides privacy and authentication of vehicles. Only legitimate vehicles are allowed in path construction. Whereas in EHACORP only the shortest path is used for data transmission. The convergence speed of F-ANT is very low, which degrades its performance in terms of throughput. The modified ACR in ELAACR has a better convergence speed compared to F-ANT.

The simulation is performed with different packet sizes such as 512, and 1024 bytes. The average throughput of the proposed ELAACR is high compared to EHACORP and F-ANT. For packets of 512 bytes, ELAACR's average throughput is 680 kbps, while EHACORP's is 640 kbps, and F-ANT records 610 kbps. For 1024 bytes of packets ELAACR's average throughput is 600 kbps, while EHACORP's is 570 kbps, and F-ANT records 550 kbps. Figures 9 and 10 depict the throughput performance of all schemes for vehicle density and packet sizes.

4.6.2 Packet Loss Rate (PLR)

Using an optimal secure path reduces PLR in the proposed ELAACR. The legitimate nodes are only considered with a secure authentication mechanism for route construction. Similarly, the ACR of ELAACR finds the optimal route in terms of distance and hop count. In ELAACR the packets are routed through an optimal secure shortest path which avoids frequent misrouting of packets to reduce PLR. In EHACORP certain modifications to the packet header can introduce modifications for source-based routing to degrade PLR. In F-ANT, the whole routing information about the network is used for packet routing. In F-ANT

Table 6 Comparison of ELAACR with existing schemes

Algorithms	Methodology	Design objective	Parameters to Pheromone		Limitations and challenges in real word deployment	Implementation scenario	Target application	Realistic traffic flow	Simulation tool
			Deposit	Update					
EHACORP	Modified ACO based on distance-calculation method and source-based routing approach	To discover the optimal shortest route with minimum hops	Distance	Distance, pheromone quantity, and evaporation rate	Limitation In high-density networks, the size of the packet header increases, which increases the path length. Long paths slow down the convergence speed of ACO. Slow convergence speed limits the performance of ACO in dense networks Challenges Securing the source node as trustworthy is a difficult task that requires appropriate security algorithms	Highway road scenario	Efficient Routing-Real city traces	Yes	NS2
F ANT	ACO and fuzzy logic-oriented decisions according to congestion, bandwidth, and signal strength	To determine the most efficient route	Distance	Distance, pheromone value, and vaporization rate	Limitation	Urban road scenario	Efficient routing-real city traces	Yes	NS2

Table 6 (continued)

Algorithms	Methodology	Design objective	Parameters to Pheromone		Limitations and challenges in real word deployment	Implementation scenario	Target application	Realistic traffic flow	Simulation tool
			Deposit	Update					
					Storing whole network information for routing reduces FANT performance. Artificial Ant's memory requirements do not support storing the entire network data for the entire routing process Challenges Limiting node failures in highway scenarios is a challenging task in FANT. FANT is not resilient to node failures				
Proposed ELAACR	Enhanced ant colony with location–aided key management scheme	To discover efficient secure paths for seamless transmission	Cost of the edge	Cost, old pheromone amount, and evaporation rate	Limitation	Highway road scenario	Efficient and secure routing-real city traces	Yes	NS2

Table 6 (continued)

Algorithms	Methodology	Design objective	Parameters to Pheromone		Limitations and challenges in real word deployment	Implementation scenario	Target application	Realistic traffic flow	Simulation tool
			Deposit	Update					
					In urban conditions, ELAACR can find the shortest routes with a large number of vehicles as hop counts, which increases the processing overhead. ELAACR is limited to highway scenarios Challenges In an urban environment, a diverse amount of vehicles imposes a high computational cost on group signature, which increases the overall overhead. Reducing overhead in urban scenarios is a challenging task for ELAACR				

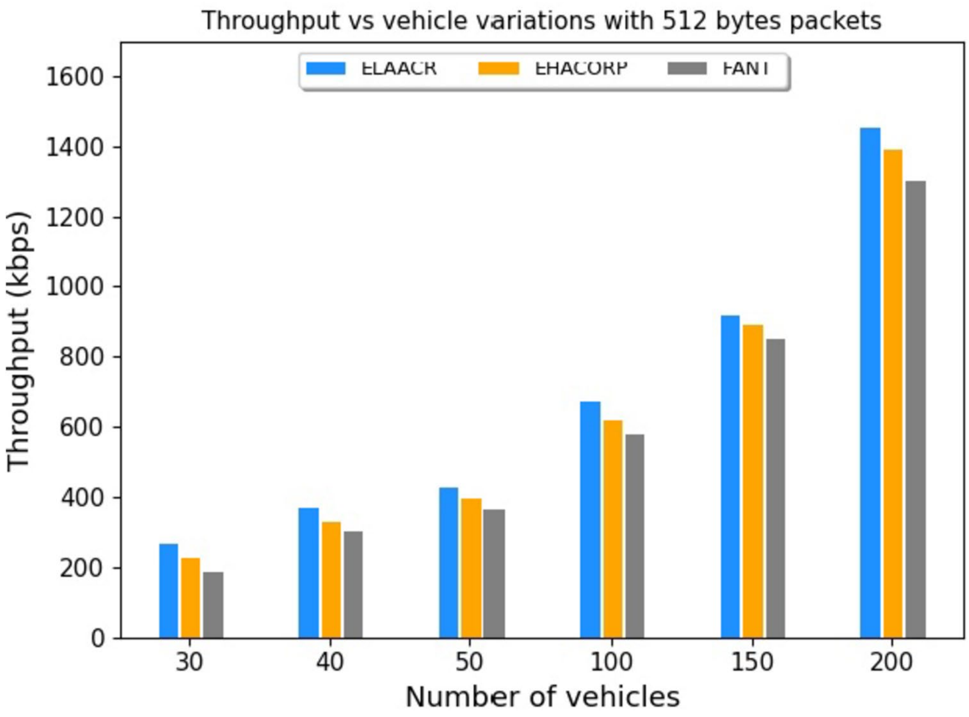


Fig. 9 Throughput at different vehicle densities for the 512 bytes packets

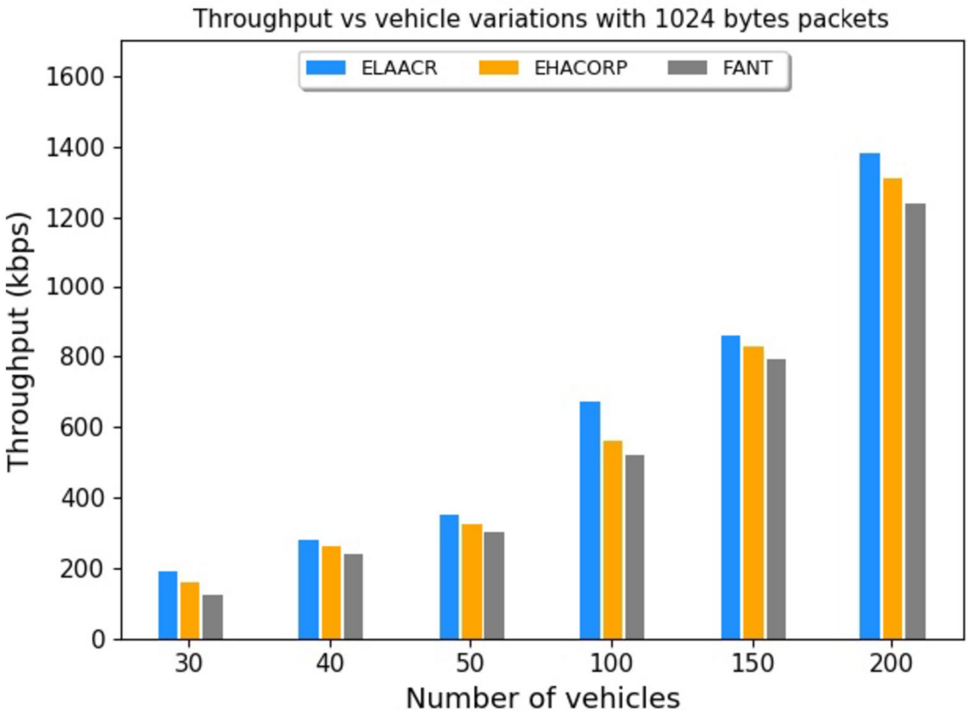


Fig. 10 Throughput at different vehicle densities for the 1024-byte packets

malicious packets can modify information in the network which improves its PLR. The secure group signature in the proposed ELAACR can avoid the misrouting of packets through malicious nodes. Similarly, the efficient paths in the proposed ELAACR provide seamless data transmission. The PLR of the introduced ELAACR is very small compared to EHACORP and F-ANT. For packets of 512 bytes, ELAACR's average PLR is 0.015%, while EHACORP's is 0.070%, and F-ANT records 0.090%. For 1024 bytes of packets ELAACR's average PLR is 0.020, while EHACORP's is 0.090%, and F-ANT records 0.102%.

Figures 11 and 12 depict the PLR performance of all schemes for vehicle density and packet sizes.

4.6.3 Packet Delivery Ratio (PDR)

In the proposed ELAACR limiting the intermediate vehicles in the path improves the packets processing time. The quick way of processing packets and using a secure path improves PDR in the proposed ELAACR. In EHACORP connection setup delay degrades its PDR. F-ANT is not able to find optimal paths for the high-density network. The accumulation of packet headers is degraded in FANT for high-density vehicles. In the ELAACR, the ACR avoids connection setup delay by using improved route finding ants.

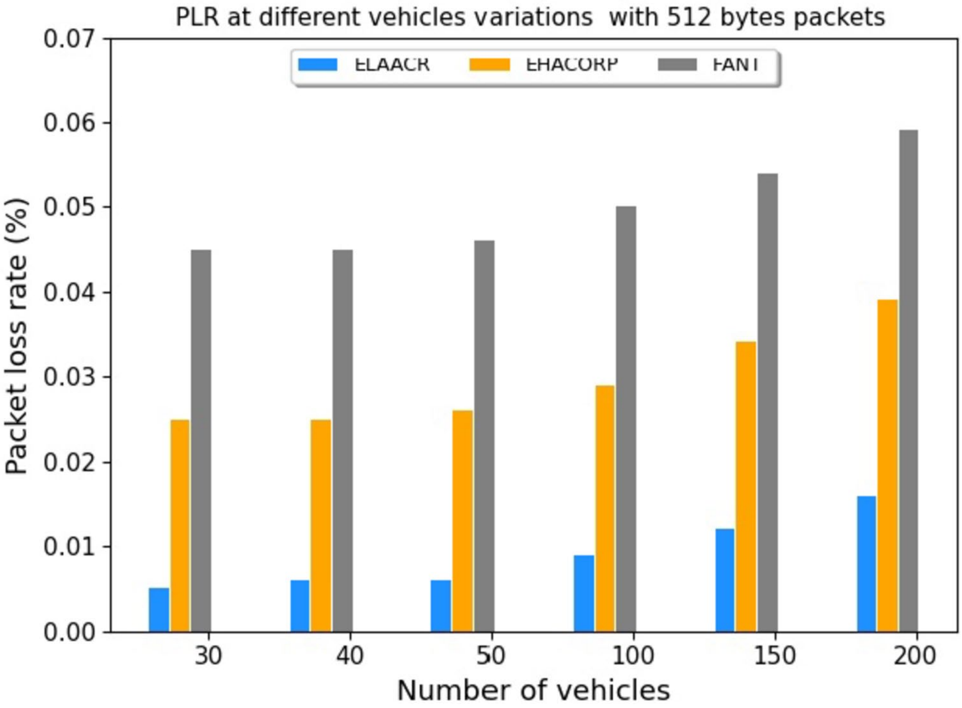


Fig. 11 PLR at different vehicle densities for the packet size of 512 bytes

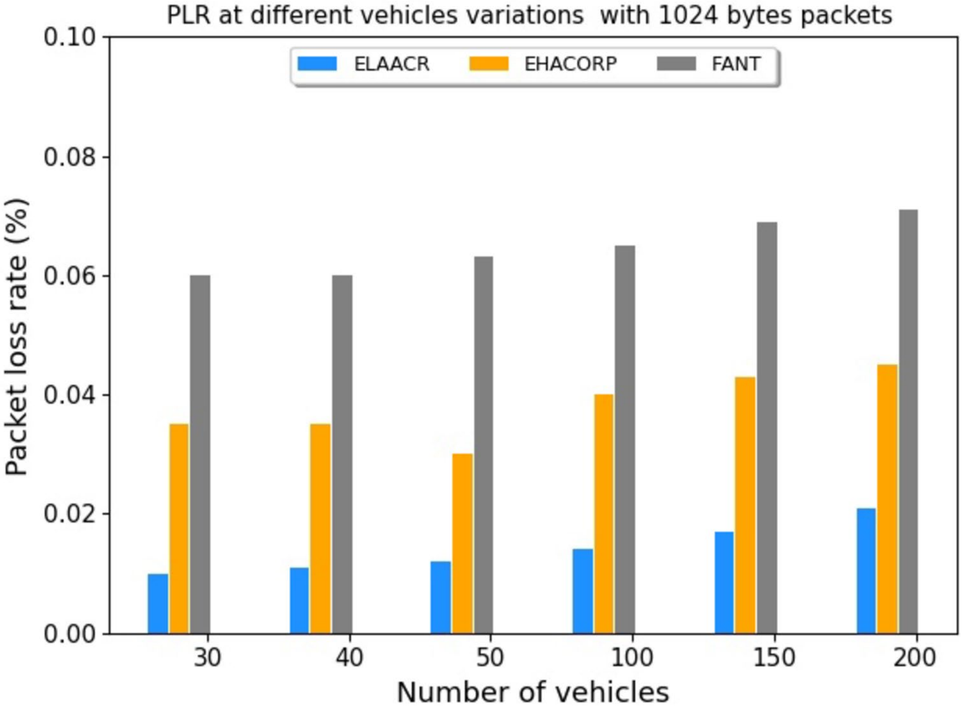


Fig. 12 PLR at different vehicle densities for the packet size of 1024 bytes

In ELAACR, REANTs reduce the complexity of the route selection procedure. The complexity level of the ELAACR for high-density networks is too low which improves its PDR. The average PDR of the proposed ELAACR is high compared to EHACORP and F-ANT. For packets of 512 bytes, ELAACR's average PDR is 98.9%, while EHACORP's is 96.1%, and F-ANT records 94.1%. For 1024 bytes of packets ELAACR's average PDR is 98.1%, while EHACORP's is 94.1%, and F-ANT records 93.0%. Figures 13 and 14 depict the PDR performance of all schemes for vehicle density and packet sizes.

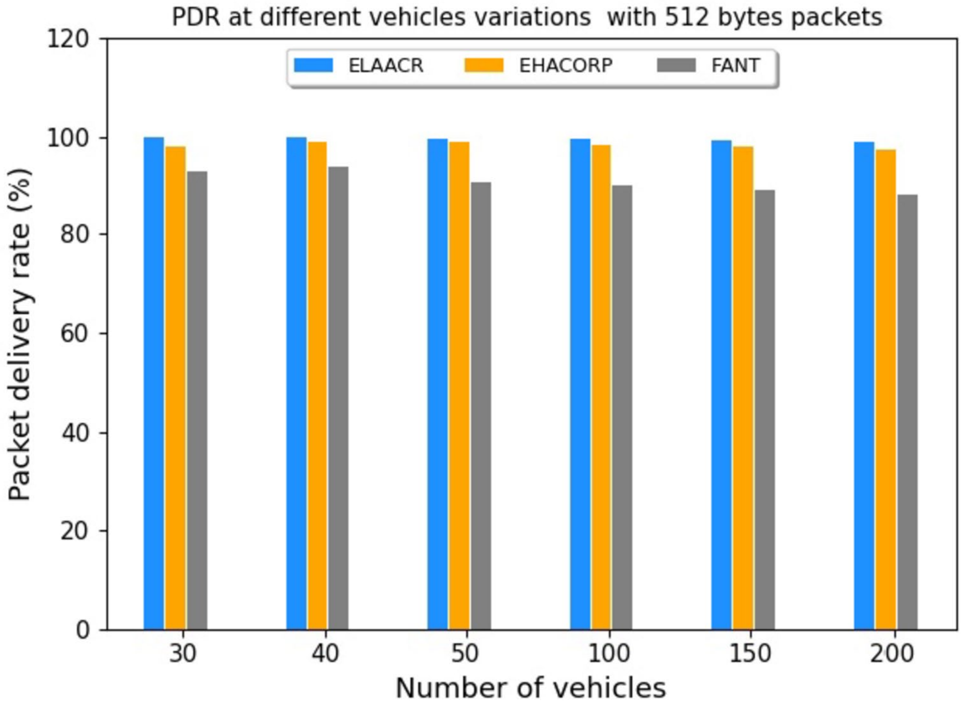
4.6.4 Overhead (OH)

Depending on minimal control packets for network management reduce OH in the proposed ELAACR. The reactive nature of the proposed ELAACR uses controlled routing packets for connection establishment and connection maintenance. In EHACORP the source-based routing is not scalable to high-density networks and demands more resources to process the packets which increases its overhead. Similarly, in FANT organizing the whole colony information in the form of updating requires more control packets. The Dynamic ACR is scalable and requires fewer resources for the speedy processing of packets. Organizing only required routing information controls overhead in the proposed ELAACR. The average OH of the projected ELAACR is small compared to EHACORP and F-ANT. For packets of 512 bytes, ELAACR's average OH is 0.145%, while EHACORP's is 0.210%, and F-ANT records 0.240%. For 1024 bytes of packets ELAACR's average PDR is 0.169%, while EHACORP's is 0.280%, and F-ANT records 0.301%. Figures 15 and 16 depict the OH performance of all schemes for vehicle density and packet sizes.

4.6.5 End-to-End Delay (EED)

Seamless data transmission in the proposed ELAACR reduces its EED. The path in the proposed ELAACR is optimal and rich in terms of short distance, security, and the number of intermediate vehicles. Controlling the path length with fewer vehicles reduces EED in ELAACR. EHACORP’s optimal route produces low EED than FANT. The slow convergence speed of FANT increases EED. Utilizing a secure shortest path with seamless data transmission reduces the EED of the proposed work. The average EED of the projected ELAACR is low compared to EHACORP and F-ANT. For packets of 512 bytes, ELAACR's average EED is 0.15 s, while EHACORP's is 0.29 s, and F-ANT records 0.59 s. For 1024 bytes of packets ELAACR's average PDR is 0.17 s, while EHACORP's is 0.40 s, and F-ANT records 0.70 s. Figures 17 and 18 depict the EED performance of all schemes for vehicle density and packet sizes.

Fig. 13 PDR at different vehicle densities for the packet size of 512 bytes



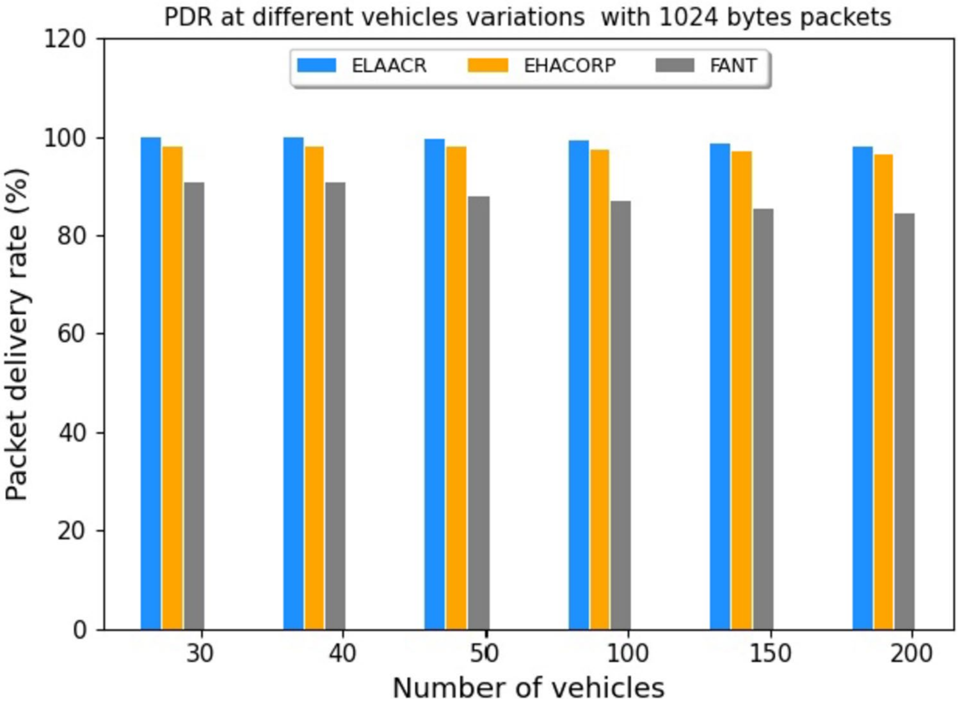


Fig. 14 PDR at different vehicle densities for the packet size of 1024 bytes

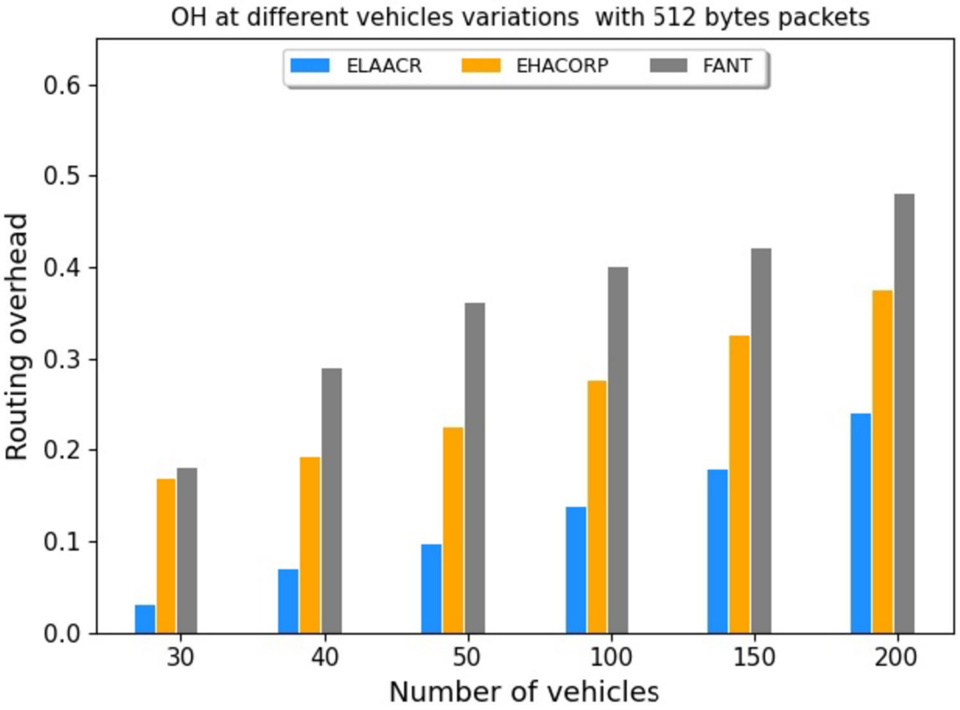


Fig. 15 OH at different vehicle densities for the packet size of 512 bytes

4.6.6 EED and PDR for Simulation Time (ST)

To check the efficiency of the proposed ELAACR against EHACORP and F-ANT whole ST is used. The Unit of time considered as ST is 500 s. The proposed ELAACR experiences better performance in terms of EED and PDR compared to EHACORP and F-ANT for the whole ST. Using a secure path with optimal connectivity enhances the PDR and EED of the proposed ELAACR. Additionally, the fast convergence speed of ACR and quick processing of all types of packets improves performance in terms of EED and PDR. Figures 19 and 20 depict the EED performance of all schemes for vehicle density and packet sizes. Figures 21 and 22 depict the PDR performance

Fig. 16 OH at different vehicle densities for the packet size of 1024 bytes

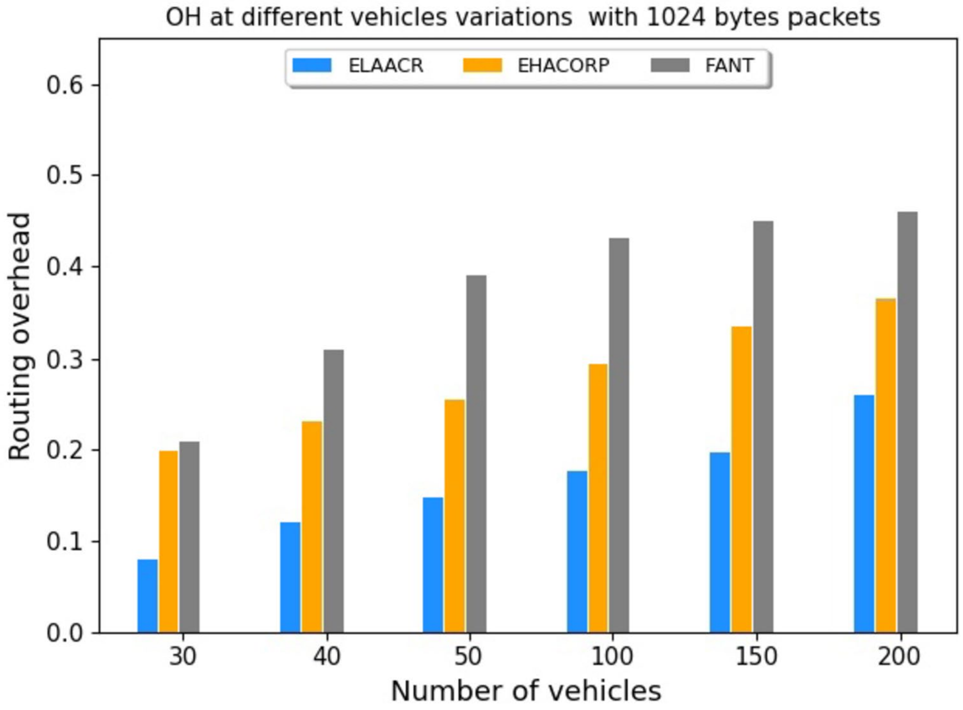
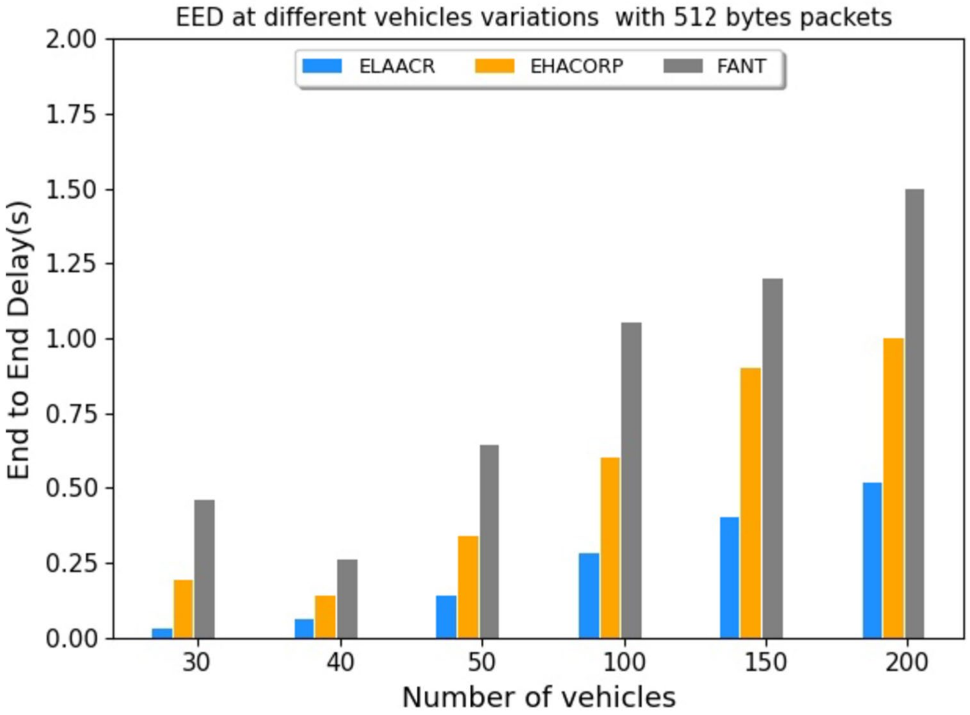


Fig. 17 EED at different vehicle densities for the packet size of 512 bytes



of all schemes for vehicle density and packet sizes. Table 7 depicts the experimental results of the proposed ELAACR, EHACORP, and F-ANT.

5 Conclusion

Information in VANETs is considered time-critical and there is a high demand for timely distribution of information about traffic, accidents, and other important information. A routing mechanism should support building

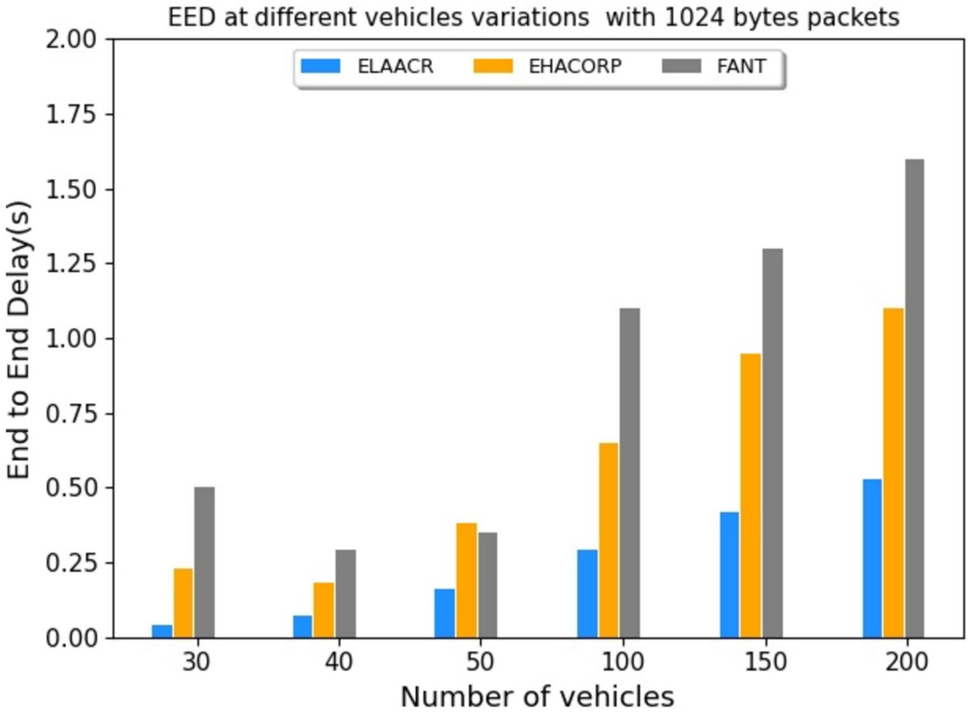


Fig. 18 EED at different vehicle densities for the packet size of 1024 bytes

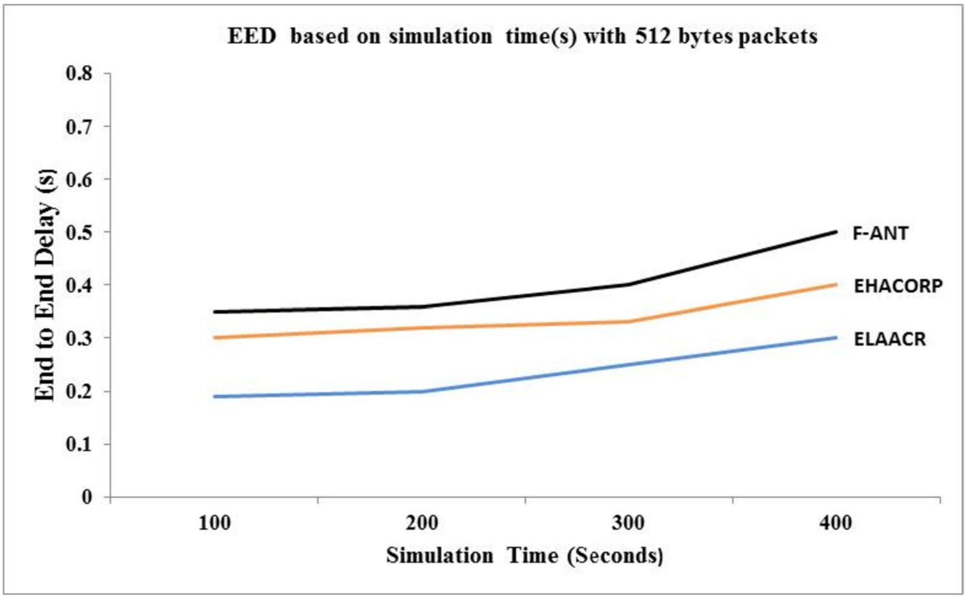


Fig. 19 EED for vehicle density with 512 bytes packets

secure seamless data transmission paths for communication between vehicles. Therefore, this work proposes ELAACR for VANETs to achieve seamless secure data transmission. The ELAACR works in two phases. In Phase 1, LAKM uses a group signature scheme to construct a secure network. Phase 2 relies on ACR to find efficient secure shortest path for seamless data transmission over a secure network. The combination of LAKM and ACR offers an efficient shortest path with low intermediate vehicles for seamless data communication. The proposed work is simulated in Network Simulator (NS 2.35).

Using a seamless secure shortest route with a restricted number of intermediate vehicles improves the throughput of the proposed ELAACR. For all data rates, the average throughput of ELAACR is 640 Kbps whereas EHACORP and F-ANT achieve 605 Kbps and 580 Kbps. Allowing only legitimate nodes through the group signature concept to construct a secure path reduces the PLR of the proposed

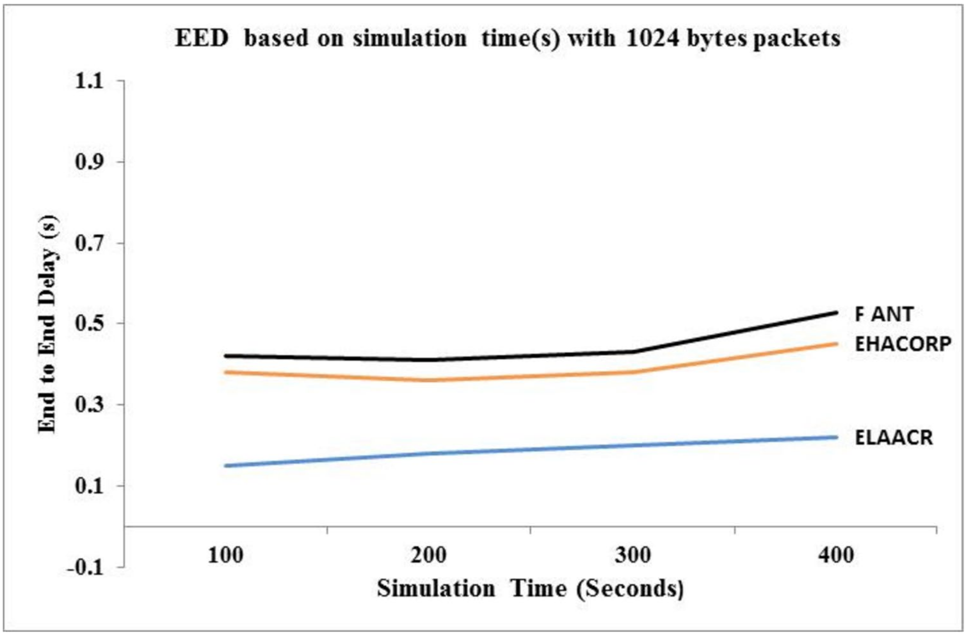


Fig. 20 EED for vehicle density with 1024 bytes packets

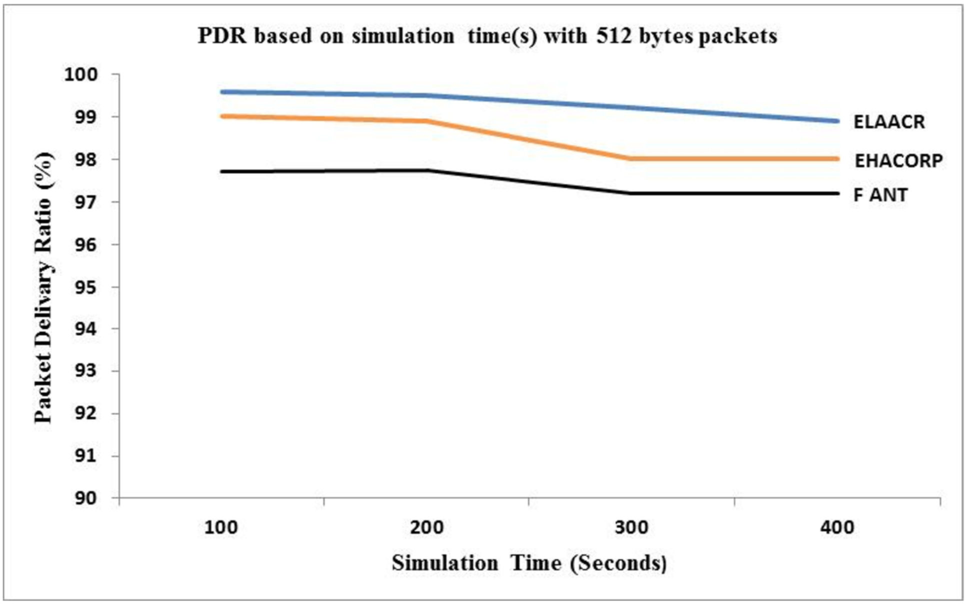


Fig. 21 PDR for vehicle density with 512 bytes packets

ELAACR. For all data rates, the average PLR of ELAACR is 0.018% whereas EHACORP and F-ANT achieve 0.080% and 0.096%. The quick delivery of packets with quick processing time improves the PDR of the proposed ELAACR. For all data rates, the average PDR of ELAACR is 98.5% whereas EHACORP and F-ANT achieve 95.1% and 93.55%. Using very limited control packets in a controlled manner improves the OH of the proposed ELAACR. For all data rates, the average OH of ELAACR is 0.157% whereas EHACORP and F-ANT achieve 0.245% and 0.270%. Seamless data transmission in the proposed ELAACR reduces its EED. The proposed ELAACR records 0.16 s whereas EHACORP and F-ANT record 0.34 s and 0. 64 s. Additionally, for ST the proposed ELAACR records good improvements. Using efficient routes for uninterrupted data transmission increases the performance of the projected ELAACR in terms of PDR and EED based on ST.

The proposed ELAACR is limited and intended to offer optimal routing for VANETs in highway scenarios. The functioning of ELAACR is to improve for urban environment to deal with significant diversities in terms of intersections, streets, traffic signals, crosswalks, buildings, etc. The availability of more obstacles affects signal transmission, which ends in non-efficient routing. The proposed ELAACR

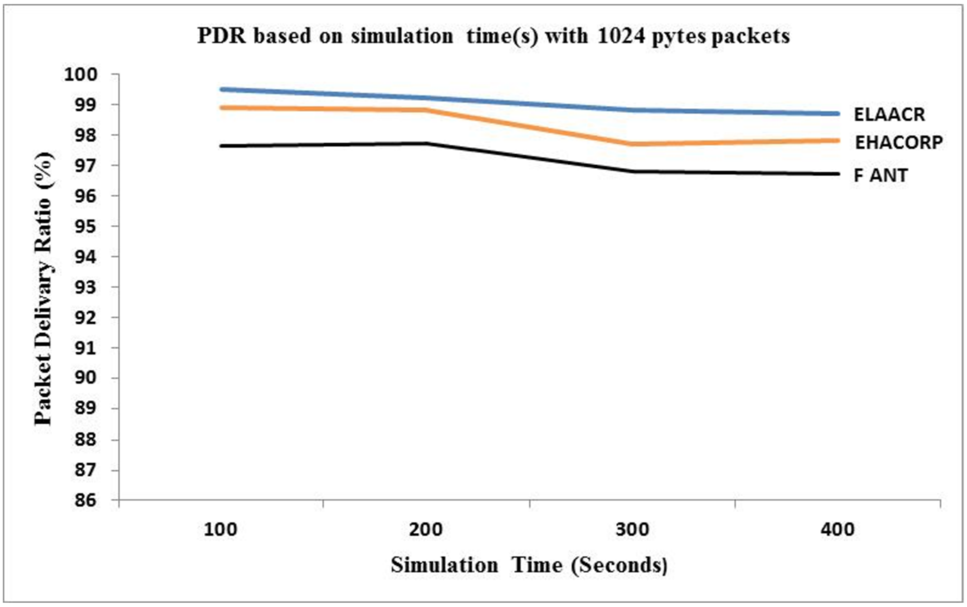


Fig. 22 PDR for vehicle density with 1024 bytes packets

Table 7 Experimental results

Parameters	Packet size in bytes	Protocols		
		ELAACR	EHACORP	F-ANT
Average T	512	680	640	610
	1024	600	570	550
Average T (Kbps) for all packet sizes		640	605	580
Average PLR	512	0.015	0.070	0.090
	1024	0.020	0.090	0.102
Average PLR (%) for all packet sizes		0.018	0.080	0.096
Average PDR	512	98.9	96.1	94.1
	1024	98.1	94.1	93.0
Average PDR (%) for all packet sizes		98.5	95.1	93.55
Average OH	512	0.145	0.210	0.240
	1024	0.169	0.280	0.301
Average OH (%) for all packet sizes		0.157	0.245	0.270
Average EED	512	0.15	0.29	0.59
	1024	0.17	0.40	0.70
Average EED (seconds) for all packet sizes		0.16	0.34	0.64
Average EED (ST)	512	0.23	0.33	0.40
	1024	0.20	0.40	0.45
Average EED (seconds) for all packet sizes based on ST		0.22	0.37	0.43
Average PDR (ST)	512	99.3	98.4	97.4
	1024	99.0	98.3	97.2
Average PDR (seconds) for all packet sizes based on ST		99.2	98.4	97.3

is limited and intended to offer optimal routing for VANETs in highway scenarios. The working method of ELAACR can be improved for urban environments with different road scenarios to deal with significant variations in terms of intersections, streets, traffic signals, crosswalks, buildings, etc. The availability of more obstacles affects signal transmission, which ends in non-efficient routing. Furthermore, the VANETs need to handle huge data on time which requires attention to congestion schemes to avoid congested routing. By considering this demand the ELAACR needs to be enhanced with congestion-oriented schemes to provide more efficient routing. Congestion models to detect congestion at the link and node levels need to be incorporated with ELAACR to improve its efficiency.

Acknowledgements The author would like to thank the management of Oxford College of Engineering for moral support during manuscript preparation.

Author Contributions RR carried out all research tasks including finding the problem, analyzing the related works, and implementing the proposed method as well as writing the manuscript.

Funding This study received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Availability of Data and Materials All data generated or analyzed during this study are included in this published article.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

Ethics Approval and Consent to Participate Not applicable.

Consent for Publication Not applicable.

References

1. Ullah S, Abbas G, Waqas M, Abbas ZH, Khan AU. RSU assisted reliable relay selection for emergency message routing in intermittently connected VANETs. Wirel Netw. 2023;29(3):1311–32.
2. Husnain G, Anwar S, Shahzad F. An enhanced AI-enabled routing optimization algorithm for internet of vehicles (IoV). Wirel Pers Commun. 2023;130(4):2623–43.
3. Gopalan SH, Ashok J, Manikandan A, Ramalingam S. Data dissemination protocol for VANETs to optimize the routing path using hybrid particle swarm optimization with sequential variable neighbourhood search. Telecommun Syst. 2023;84(2):153–65.
4. Ramamoorthy R, Kumar S, Naidu RCA, Sathya M. Hybrid multihop routing mechanism with intelligent transportation system architecture for efficient routing in VANETs. In: *2022 international conference on disruptive technologies for multi-disciplinary research and applications (CENTCON)*, vol. 2. New York: IEEE; 2022, December. p. 69–74.
5. Kadam MV, Vaze VM, Todmal SR. TACR: trust aware clustering-based routing for secure and reliable VANET communications. Wirel Pers Commun. 2023;132(1):305–28.
6. Ramamoorthy R, Thangavelu M. Group-based dual mode key management scheme for secure communication in vehicular ad hoc networks. Wirel Pers Commun. 2021;120:949–73.
7. Harrabi S, Jaafar IB, Ghedira K. Survey on IoV routing protocols. Wirel Pers Commun. 2023;128(2):791–811.
8. Ikhlef H, Bourebia S, Melit A. Link state estimator for VANETs using neural networks. J Netw Syst Manag. 2024;32(1):10.
9. Raghu R, Menakadevi T. A survey on anonymous secure on-demand routing protocols in MANETs. Middle East J Sci Res. 2016;24:3869–80.
10. Muniyandi RC, Qamar F, Jasim AN. Genetic optimized location aided routing protocol for VANET based on rectangular estimation of position. Appl Sci. 2020;10(17):5759.
11. Reka R, Manikandan A, Venkataramanan C, Madanachitran R. An energy efficient clustering with enhanced chicken swarm optimization algorithm with adaptive position routing protocol in mobile adhoc network. Telecommun Syst. 2023;84(2):183–202.
12. Raghu R, Prabhushankar R, Rajaram J, Vaiyapuri M. Efficient dead reckoning approach for localization prediction in VANETs. J Appl Sci Comput. 2019;6(3):2093–9.
13. Gurumoorthi E, Ayyasamy A. Cache agent based location aided routing using distance and direction for performance enhancement in VANET. Telecommun Syst. 2020;73(3):419–32.
14. Pandey K, Raina SK, Raw RS. Distance and direction-based location aided multi-hop routing protocol for vehicular ad-hoc networks. Int J Commun Netw Distrib Syst. 2016;16(1):71–98.
15. Ali ZH, Zaki JF, El-Rashidy N. Dynamic urban evaluation routing protocol for enhanced vehicle ad hoc networks. J Supercomput. 2023;79(6):6017–39.
16. Karp B, Kung, HT. Gpsr: greedy perimeter stateless routing for wireless networks. In: Proceedings of the MobiCom'00, Boston, MA, USA; 2000. p. 243–54.
17. Aluvala S, Rajasekhar K. Secure routing in MANETS using adaptive cuckoo search and entropy based signature authentication. Wirel Pers Commun. 2023;128(3):1519–41.
18. Sudarsono A. An implementation of efficient group signature for anonymous authentication system in vehicular ad-hoc networks. In: *2020 international electronics symposium (IES)*. New York: IEEE; 2020, September. p. 108–15.
19. Funderburg LE, Lee IY. Efficient short group signatures for conditional privacy in vehicular ad hoc networks via ID caching and timed revocation. IEEE Access. 2021;9:118065–76.
20. Lu Y, Cao S, He Q, Fang Z, Yan J, Guo Y. Group signature authentication scheme with credit evaluation mechanism in VANET. In: 2023 26th international conference on computer supported cooperative work in design (CSCWD). IEEE; 2023, May, pp. 1703–9.
21. Li S, Yang R, Chen J. A privacy-preserving authentication scheme for VANETs with exculpability. Secur Commun Netw. 2023;2023:12. https://doi.org/10.1155/2023/8676929. (**Article ID 8676929**).
22. Zhang X, Lai J, Moshayedi AJ. Traffic data security sharing scheme based on blockchain and traceable ring signature for VANETs. Peer Peer Netw Appl. 2023;16(5):2349–66.
23. Liu X, Yang Y, Xu E, Jia Z. An authentication scheme in VANETs based on group signature. In: Intelligent computing theories and application: 15th international conference, ICIC 2019, Nanchang, China, August 3–6, 2019, proceedings, part I 15. London: Springer; 2019. p. 346–55.
24. Cahyadi EF, Su TW, Yang CC, Hwang MS. A certificateless aggregate signature scheme for security and privacy protection in VANET. Int J Distrib Sens Netw. 2022;18(5):15501329221080658.
25. Lim K, Liu W, Wang X, Joung J. SSKM: Scalable and secure key management scheme for group signature based authentication and CRL in VANET. Electronics. 2019;8(11):1330.
26. Chhikara P, Patel AK. Enhancing network security using ant colony optimization. Global J Comput Sci Technol Netw Web Secur. 2013;13(4):19–22.
27. Saleem K, Ahmad I. Ant colony optimization ACO based autonomous secure routing protocol for mobile surveillance systems. Drones. 2022;6(11):351.

28. Zhang H, Bochem A, Sun X, Hogrefe D. A security aware fuzzy enhanced ant colony optimization routing in mobile ad hoc networks. In: 2018 14th international conference on wireless and mobile computing, networking and communications (WiMob). IEEE; 2018, October. p. 1–6.
29. Ramamoorthy R, Thangavelu M. An enhanced distance and residual energy-based congestion aware ant colony optimization routing for vehicular ad hoc networks. Int J Commun Syst. 2022;35(11):e5179.
30. Maranur JR, Mathapati B. ARPVP: attack resilient position-based VANET protocol using ant colony optimization. Wirel Pers Commun. 2023;128(2):1235–58.
31. Patel KN, Jhaveri RH. Isolating packet dropping misbehavior in VANET using ant colony optimization. Int J Comput Appl. 2015;120(24):1.
32. Anantapur M, Patil VC. Ant colony optimization based modified AODV for secure routing in mobile ad hoc networks. Int J Intell Eng Syst. 2021;14(6):115–24.
33. Maheshwari S, Bhardwaj M. Secure route selection in MANET using ant colony optimization. Am J Netw Commun. 2015;4(3–1):54–6.
34. Ramamoorthy R, Thangavelu M. An improved distance-based ant colony optimization routing for vehicular ad hoc networks. Int J Commun Syst. 2020;33(14):e4502.
35. Ramamoorthy R, Thangavelu M. An enhanced bio-inspired routing algorithm for vehicular ad hoc networks. Trends Sci. 2022;19(10):4188–4188.
36. Ramamoorthy R, Thangavelu M. An enhanced hybrid ant colony optimization routing protocol for vehicular ad-hoc networks. J Ambient Intell Hum Comput. 2021;13:3837–68.
37. Fatemidokht H, Kuchaki Rafsanjani M. F-Ant: an effective routing protocol for ant colony optimization based on fuzzy logic in vehicular ad hoc networks. Neural Comput Appl. 2018;29:1127–37.
38. Deshmukh AR, Nirmal P, Dorle SS. A new approach for position-based routing protocols based on ant colony optimization (ACO) technique in vehicular ad hoc network (VANET). In: 2021 international conference on intelligent technologies (CONIT). IEEE; 2021, June. p. 1–5.
39. Ebadi Y, Jafari Navimipour N. An energy-aware method for data replication in the cloud environments using a Tabu search and particle swarm optimization algorithm. Concurr Comput Pract Exp. 2019;31(1):e4757.
40. Lee KY, Vlachogiannis JG. Ant colony optimization for active/reactive operational planning. IFAC Proc Vol. 2005;38(1):97–102.
41. Janakiraman S. A hybrid ant colony and artificial bee colony optimization algorithm-based cluster head selection for IoT. Proc Comput Sci. 2018;143:360–6.
42. Sharma I, Ramkumar KR. A survey on ACO-based multipath routing algorithms for ad hoc networks. Int J Pervasive Comput Commun. 2017;13(4):370–85.
43. Rupérez Cañas D, Sandoval Orozco AL, García Villalba LJ, Kim TH. A family of ACO routing protocols for mobile ad hoc networks. Sensors. 2017;17(5):1179.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.